NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

EXPLORING THE STRUCTURE AND TASK DYNAMICS OF TERRORIST ORGANIZATIONS USING AGENT BASED MODELING

by

Nikolaos Bekatoros

December 2008

Thesis Co-Advisors: Mark E. Nissen
Erik Jansen

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2008	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Exploring the Structure and Task Dynamics of Terrorist Organizations Using Agent Based Modeling		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Nikolaos Bekatoros			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

This thesis examines the structure and attributes of the terrorist network that was responsible for the 2004 Madrid bombing attack. It initially produces a Baseline computational model using POW-ER, based on data from academic papers and news articles about the 2004 Madrid bombings. The Baseline model is further compared with two different representations of the same terrorist group: 1) the Expert model, which is identical to the Baseline model except for the fact that the actors have high application experience and skill levels, and 2) the Hierarchical model, which is similar to the Baseline but with a hierarchical structure. All models are tested under both baseline and high counterterrorist conditions. This thesis examines how different contingency factors affect the preparation and execution of a terrorist bombing attack and provides recommendations to inform counterterrorist agencies.

.

14. SUBJECT TERMS Terrorist Networks, Agent Based Modeling, 2004 Madrid Attacks, Backcasting, Computational Organization Simulation			**15. NUMBER OF PAGES** 75
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

EXPLORING THE STRUCTURE AND TASK DYNAMICS OF TERRORIST ORGANIZATIONS USING AGENT BASED MODELING

Nikolaos Bekatoros
Lieutenant Junior Grade, Hellenic Navy
B.S., Hellenic Naval Academy, 2000

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION WARFARE SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
December 2008

Author: Nikolaos Bekatoros

Approved by: Mark E. Nissen
Thesis Co-Advisor

Erik Jansen
Thesis Co-Advisor

Dan C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis examines the structure and attributes of the terrorist network that was responsible for the 2004 Madrid bombing attack. It initially produces a Baseline computational model using POW-ER, based on data from academic papers and news articles about the 2004 Madrid bombings. The Baseline model is further compared with two different representations of the same terrorist group: 1) the Expert model, which is identical to the Baseline model except for the fact that the actors have high application experience and skill levels, and 2) the Hierarchical model, which is similar to the Baseline but with a hierarchical structure. All models are tested under both baseline and high counterterrorist conditions. This thesis examines how different contingency factors affect the preparation and execution of a terrorist bombing attack and provides recommendations to inform counterterrorist agencies.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

One of the premier issues facing governments today is terrorist networks. These networks must be understood in order to apply effective policies and practices to safeguard citizens, assets, and interests. For decades, terrorist cells have relied on the support provided by structured organizations like Al Qaeda for their funding, planning and execution of attacks (Benjamin & Simon, 2005). However, recent large-scale terrorist acts, like the Madrid bombings in 2004 or the London bombings in 2005, strengthen the view that terrorist cells operate in a self-organized manner (Benjamin & Simon, 2005; Bell, 2002).

On Thursday, March 11, 2004 at 0639 GMT, within a three-minute time frame, ten bombs exploded on four trains in three stations in Madrid, Spain (BBC News, March 12, 2004). This attack killed 191 people and wounded 1800 more (Jordan & Wesley, 2006). The attack occurred three days before the general elections. Euskadi Ta Askatasuna (ETA), a terrorist group that has performed many terrorist attacks on Spanish soil since it was founded in 1959, was blamed by the Popular Party's Prime Minister José Mariá Aznar for being responsible for these attacks, even though early findings suggested that ETA's "methods" did not match with those used by the terrorists who had performed the 2004 Madrid bombings.

After a few days, it became clear from the emerging evidence that a Jihadi terrorist group was responsible for the attacks (Benjamin & Simon, 2005; Wright, 2004). The Spaniards were angry with the Popular Party, both for insisting that ETA was involved in the attacks and for sending Spanish troops to Iraq despite the public's negative opinion of this act. The terrorists who had performed the attacks demanded the removal of Spanish troops from Iraq. The Socialist Party, which had been promising the removal of troops from Iraq in its recent campaign, was elected at the general elections on March 14, 2004, and Spain withdrew its troops from Iraq (Benjamin & Simon, 2005).

Many academics and practitioners have suggested counterterrorist policies that could be adopted by governments. Bell (2002) writes that thwarting terrorism requires a policy that focuses on the idea that, because terrorism relies on commitment, "loss of faith, the imposition of reality, and changing times can erode its strength." Changes in the Islamic population's ideological and cultural beliefs about Western culture may diminish the motivation of people to join terrorist groups. This change of ideology may be achieved by developing a higher standard of living in regions that "generate" terrorists (Brafman & Beckstrom, 2006).

Loss of faith and imposition of reality are two issues that require time. The near term issue that arises is how terrorist networks can be understood and more effectively thwarted until Bell's policy reaches its goal?

Network theory, a branch of complexity theory, tries to explain the various types of systems that emerge in the real world. It is based on mathematical graph theory. Networks can be divided into four components: social (among people or groups of people), information or knowledge (such as the network of citations among academic papers), technological (such as the electric power grid) and biological (such as DNA) (Newman, 2003).

In order to understand terrorist networks, many analysts use the Social Network Analysis approach (Hassan, 2007; Mccartan et al., 2008; Magouirk et al., 2008; Jordan et al., 2008). Social Network Analysis examines the connections and interactions among individuals or groups based on common patterns of friendship, occupation, ethnicity, or any other pattern that is of interest to the researcher (Newman, 2003). Hence, terrorist networks are analyzed in terms of variables such as strong and weak ties, and density among the participants or groups that constitute the network.

Traditional social network studies often have been criticized for inaccuracy and subjectivity (Newman, 2003). Even though many of these studies follow a backwards approach (Burton, 2003) after the events under examination have occurred (Hassan 2007; Mccartan et al., 2008; Jordan et al., 2008), the created networks may be inaccurate because of vital data missing from the researcher's database. The reasons for this missing

data could be because some information was confidential, some information never was publicly released, or because the network included participants who were not considered to be a part of this network. Of course, many social network analysis papers take these considerations into account (Mccartan et al., 2008; Jordan et al., 2008). Moreover, Social Network Analysis does not examine the structure or the workflow of a network for specific activities (e.g., a bombing attack) or the types of interdependencies (pooled, sequential, and reciprocal (Thompson, 1967) that exist among the tasks.

According to Simon (1993) and Epstein (1999), emerging virtual environments based on computational models can imitate actions and behaviors observed in the real world. It must be kept in mind that "we do not have to know, or guess at, all the internal structure of the system but only that of it that is crucial to the abstraction" (Simon, 1996). Conceptual Simulation Models have been used to represent terrorist networks as a business process and provide insights to counterterrorism policy makers (Nissen & Leweling, 2007). These computer-based models analyze terrorist networks primarily through the lens of contingency theory using Agent Based Modeling techniques.

The examination of terrorist networks from an organizational point of view has been criticized because terrorist networks cannot be seen as a part of a larger terrorist network; they operate in a self-organizing way and the network's participants constantly change (Bell, 2002; Benjamin & Simon, 2005). However, locally autonomous terrorist groups that are task oriented meet Galbraith's (1977) definition of organization: they are composed of groups of people in order to achieve their purpose (the terrorist attack) through a division of labor among the network's participants. These groups are integrated by information-based decision processes that are continuously performed by the network's participants. Sequential tasks are performed as in a typical assembly line. The output of task A is the input of task B, where task A is B's preceding task. Although task B depends on task A, task A is not dependent on task B. Reciprocally interdependent tasks are performed together, and the output of a task becomes the input of another task and vice versa (Thompson, 1967). For example, a terrorist attack can be divided into distinct sequential tasks (e.g., plan, finance, assemble the explosives, train, and execute) but some tasks are also reciprocally interdependent (e.g., the planning and financing

phases of a terrorist attack, after a certain point, are performed together and a change of the output of one task directly affects the input of the other). Bell's (2002) view of locally autonomous terrorist networks works in organization theory because "organizations seek to place reciprocally interdependent positions tangent to one another, in common group which is (a) local and (b) conditionally autonomous" (Thompson, 1967).

Tasks that require reciprocal interdependence need to be coordinated mutually by the participating members. The required amount of coordination among the members of terrorist networks is largely due to the low level of experience among their members (the Madrid terrorist cell) and the complexity involved in performing a terrorist act under secrecy. As a result, the members of terrorist networks rely on project grouping to accomplish the required coordination (Thompson, 1967).

This thesis examines the structure and attributes of the terrorist network responsible for the bombing attack that occurred in Madrid on March 11, 2004. The intent is to represent the terrorist network responsible for the Madrid Attack and examine the key attributes of this network. Emphasis is placed on the actors' roles, which will be examined with the use of computer simulation. The data set is drawn from many academic papers and news articles that analyze or describe this specific event. This thesis focuses on the exploration of the structural and task dynamics of the network using Agent Based Modeling (Epstein & Axtell, 1996; Miller & Page, 2007). The research question is: How do different contingency factors affect the preparation and execution of a terrorist bombing attack? These contingency factors are the structural configuration of the terrorist network, the environmental ambiguity and complexity, and the members' skill level. The selection of the case study approach is based on the research question. According to Yin (2002), a case study is appropriate when "a 'how' or a 'why' question is been asked about a contemporary set of events, over which the investigator has little or no control."

This thesis produces a computational model using Agent Based Modeling software POW-ER v.3.5b, which imitates the structure and the workflow of the terrorist network before the attack (Baseline model). A cross comparison of the generated computer model with Social Network Analysis representations that describe the Madrid attack and the existing datasets is made in order to evaluate the validity of the model.

Hence, keeping a balanced level of realism in the construction of the computational model, this thesis examines and analyzes the process of the Madrid terrorist attack, suggesting counterterrorism policies.

Sensitivity analysis of the computational model can identify those "parameters and relationships to which the behavior and policy recommendations are sensitive" (Sterman, 2000). According to Galbraith (1977), a low level of formalization can handle high uncertainty. In addition, experienced workers produce fewer exceptions than inexperienced ones in unstable environments. The Madrid terrorist network had low formalization and centralization (Benjamin & Simon, 2005) and the members' skill level was low. According to Haahr-Escolano (2005), the members of the 2004 Madrid cell were "amateurs." In addition, the Madrid network was highly decentralized (Benjamin & Simon, 2005). Galbraith (1977) proposed that, when the tasks performed by a hierarchical organization become complex and unpredictable, then senior managers are overloaded with exceptions. An exception occurs when there is lack of information at the responsible node to accomplish a task. Therefore, this thesis compares the Baseline model with both an "Expert" model, which is the same as the baseline model with the difference that its members have high skill and application experience levels, and with a "Hierarchical" model, which was built based on the Baseline model, under different counterterrorist environments. According to Burton & Obel (1995), computational models can be used to examine "what is," "what if," and "what should be" questions. This thesis initially examines the "what is" question with the baseline model based on archival data about the 2004 Madrid bombings, and afterward compares the Baseline model with the two other hypothetical models in order to test the "what if" question. This approach is used in order to examine how different contingency factors affect the preparation and execution of a terrorist bombing attack, which is the research question of this thesis. The results of these comparisons also suggest potential policies and actions that could slow down or disrupt terrorist networks. This thesis also shows how a computational modeling technique like Agent Based Modeling is able to examine specific terrorist attacks, and provide counterterrorist recommendations using real world data.

The second chapter covers the theoretical background on Network Theory, Organization Design, and Computer Simulation. The next chapter covers the case study of the 2004 Madrid bombings. The fourth chapter covers the research design of the thesis. The fifth chapter has the results of the various simulations and comparative presentations of the findings. The last chapter covers the findings, the limitations of this thesis, suggests counterterrorism policies, and indicates potential venues for future research.

II. BACKGROUND

This section initially examines terrorism in general, and it covers some additional background about the way it is viewed in the information age. Then it analyzes the Social Network Analysis (SNA) technique that is used by scholars and practitioners in order to analyze terrorist networks. SNA is a branch of network theory that has its roots in graph theory from mathematics, so a brief description of network theory also is provided. The purpose of this thesis is to examine the process and the contingency factors that affect the development of a terrorist bombing "project," using existing data from the March 11, 2004 Madrid bombings. This examination is performed with the use of computational models, so a brief description of computational organization theory is provided.

A. TERRORISM AS A FORM OF WARFARE IN THE INFORMATION AGE

Many scholars have defined terrorism, and its definition has been a point of contention within academia. The difficulty with terrorism is that, even though it is an "ism" (like communism, capitalism or even postmodernism), it does not represent an ideological, political or cultural category. Terrorism is a tactic where fear is the dominant key element. Other key elements of terrorism are the use of violence, the symbolic use of victims, the absence of moral constraint, advanced planning and operational seriality (Robb, 2007).

Terrorism is a tactic, and tactics are parts of warfare. According to Robb (2007), there are four generations of warfare. The first two generations of warfare (Mass and Industrial) are considered as conventional warfare, and the second two generations (Blitzkrieg & Guerilla) as unconventional warfare. Conventional warfare is the type of warfare that is fought between nations, where the conflict takes place among well-structured armies following tactics and procedures. In conventional warfare, armies traditionally target only what is of military interest. In contrast to conventional warfare, unconventional warfare uses indirect opposition tactics and is based on surprise and low intensity conflicts. In unconventional warfare, civilians and noncombatant infrastructures

may be targeted on purpose by the opposing groups. A commonly used method is the "system disruption method," which is a simple way of attacking the critical networks (electricity, oil, gas, water and communications) that underpin social life.

Terrorism could fit in the fourth generation of warfare (guerilla warfare), since it has many elements in common. On the other hand, terrorism has some critical differences with guerilla warfare that make it distinct. Guerillas use terror to influence the noncombatant population, and their tactics are similar to the ones used by terrorists. The differences with guerilla warfare are the following: (a) terrorist groups operate globally and are not limited within the borders of a particular country like guerillas; and (b) a guerrilla tries to destabilize a particular state, but terrorism has as a goal to destabilize a series of countries, mainly the Western ones (Wright, 2004). In addition, terrorism operates in both the physical and information domain, while guerillas operate mainly in the physical domain (Robb, 2007). Hence, terrorism is a distinct form of warfare. Therefore, like any "age," the information age has its own form of war (Arquilla, 1996).

Al Qaeda (AQ) is the largest terrorist organization with multiple cells and affiliates in existence and has been responsible for major terrorist attacks (New York, 2001, Bali, 2002, Madrid, 2004, London, 2005). It was founded after the Soviet invasion of Afghanistan as an anti-Soviet resistance organization. At that time, it was an army of Arab warriors who entered the war in order to help the Afghans fight the Soviets, and it was known to the world as the anti-Soviet jihad (Napoleoni, 2005).

There are two kinds of jihad: defensive and offensive. The defensive jihad is about taking up arms in order to protect Islam, and the offensive one is about taking up arms for spreading Islam. In order to perform offensive jihad, the emir or caliph of the community should call for arms and it is then the duty of all Muslims to join him. Osama Bin Laden and other leaders of Islamic organizations like Al Zarqawi (Napoleoni, 2005) took the emir's role in Al Qaeda. Blind terrorist hits have been made in the name of jihad, including the March 11, 2004 Madrid bombing attacks (Wright, 2004; Benjamin & Simon, 2005).

After the Soviets left Afghanistan in 1989, AQ remained active, and was transformed into a terrorist organization. The anti-Soviet jihad was transformed by its leaders into an anti-colonization jihad. The organization configuration of Al Qaeda in the late 1990s was bureaucratic (Mintzberg, 1980), and was commonly referred to as a hierarchy (Benjamin & Simon, 2005). The organization was established in Afghanistan and had its training camps across the country. Al Qaeda's leader was Osama Bin Laden, and beneath him, there was a clear hierarchical structure.

After 9/11 and the beginnings of the wars in Afghanistan and Iraq, AQ decentralized and its cells were spread across the world, enforcing the existing ones or creating new ones. AQ is a network of networks. Small terrorist organizations that operate in various countries are interconnected into a larger network that forms the Al Qaeda organization (Benjamin & Simon, 2005).The structure of this terrorist network is not hierarchical or close to any of Mintzberg's organizational configurations (Bell, 2002). Al Qaeda's new organizational configuration can be characterized as an Edge organization (Alberts & Hayes, 2003). The Al Qaeda network contains decentralized teams that operate within complex environments with great agility and adapt to the emerging interchanging conditions. The leader of Al Qaeda is still Osama Bin Laden, but his role is more ideological and is accomplished by spreading videos and declarations; he has no managerial role in coordinating the existing terrorist branches of Al Qaeda (Wright, 2004; Wiemann, 2006).

According to Robb (2006), each state's goal is to control the economy, resources, laws, infrastructure, education and health of its citizens. Terrorists' desire is a failed state. They believe that, if the state fails, they win. Moreover, technology is advancing rapidly, providing power to non-state actors, and this growth strengthens the ability of groups to use decentralized technological tools in order to attack a state. The Global War on Terror (GWOT) is a decentralized war where small groups have a dominant role.

B. NETWORK THEORY AND SOCIAL NETWORKS

In order to thwart terrorism groups, many researchers and practitioners analyze the structure of terrorist networks using Social Network Analysis (SNA), a technique that

is based on network theory (Magouirk et al., 2008; Jordan et al., 2008). SNA deals with the analysis of the structure of social networks. A network is a set of nodes that are interconnected in a specific way with links. Links represent a relation between two nodes that is based on some common characteristic (Newman, 2003). For example, links in social networks can be family relations, friendship ties or education ties. As was mentioned in Chapter I, networks can be divided into social (among people or groups of people), information or knowledge (such as the network of citations among academic papers), technological (such as the electric power grid) and biological networks (such as DNA) (Newman, 2003).

Network theory suggests three main categories of networks based on their behavior and structure. Random networks are the networks that are created by luck rather than design (Atkinson & Moffat, 2005). Scale free networks are networks, like the internet, where the hubs (nodes with a large number of links) are more likely to attract new nodes than the nodes with fewer links (Newman, 2003). These networks seem to follow the 80/20 rule, which indicates that 80 % of the network's total number of links are connected to a small number of nodes (Barabási, 2002). Small world networks are the networks where each node is connected with any other node in the network by a short path (Newman, 2003). The difference between random and small world networks is that the average path length (the average distance between a random pair of nodes) is smaller, and the clustering coefficient (how tightly the nodes are interconnected locally) is higher in small world networks (Atkinson & Moffat, 2005).

Granovetter (1973) suggested the existence of strong and weak ties within social networks. Strong ties create small worlds (clutters of nodes highly interconnected), and weak ties are the "bridges" among various small worlds. A study conducted by Milgram and Travers in 1969 was the first experimentation on social small world networks. The researchers asked 300 residents of Nebraska, USA to send a letter to a person who lived in Boston, Massachusetts, USA by way of acquaintances. A sender's friend was regarded as a first degree of separation, a friend's friend as a second and so on. This experiment showed that there were about six degrees of separation on average between the senders

and the recipient, meaning that there was a short path connecting every pair. This study has been repeated with instant messages with millions of participants in 2008 and showed results similar to Milgram's study (Yahoo News, August 4, 2008).

Social Network Analysis analyzes real world social networks based on the concept of small worlds. This technique examines the connections and interactions among individuals or groups based on common patterns of friendship, occupation, ethnicity, or any other pattern that is of interest to the researcher (Newman, 2003). The Social Network Analysis approach has been used for the study of terrorist networks (Hassan, 2007; Mccartan et al., 2008; Magouirk et al., 2008; Jordan et al., 2008). Hence, terrorist networks are analyzed in terms of variables like centrality (a high number of links constitute a central node or hub), path length (the average distance between a random couple of nodes) and the clustering coefficient (how tightly the nodes are interconnected locally).

Most academic papers that use SNA to examine terrorist networks focus on case studies that examine specific terrorist events, or explore the evolution of a terrorist network using archival data. In order to perform this analysis, the researcher ideally is fully aware of the participants of the network and their in-between relations. However, the researcher's dataset might miss vital information due to the existence of classified information or due to incomplete awareness of the complete network. Traditional social network studies have often been criticized for inaccuracy and subjectivity for the reasons mentioned above (Newman, 2003). Another limitation of SNA is that it focuses mainly on the participants and their connections, and not on the process participants perform their assigned tasks.

C. THE ORGANIZATIONAL VIEW OF TERRORIST NETWORKS

According to Benjamin & Simon (2005) and Bell (2002), terrorist cells cannot be seen as a part of a larger terrorist network like Al Qaeda because they operate locally and autonomously and the network's participants constantly change. In order to approach terrorist cells from an organizational view point, the locally autonomous terrorist cell can be considered as an organization for a short period of time when the examined network

performs a specific project (i.e., executes an attack). This approach examines terrorist cells at the group level of analysis for a short period of time, minimizing the fluidal participation that occurs within terrorist networks.

According to Galbraith (1977), "organizations are 1) composed of people and groups of people 2) in order to achieve some shared purpose 3) through a division of labor 4) integrated by information-based decision processes 5) continuously through time." The terrorist network responsible for the March 11, 2004 Madrid attacks can be identified as an organization because:

- The terrorist cell was composed of different individuals and groups of people (like the Spaniards who provided the explosives or the Moroccan drug smugglers who financed the attack);
- All group members operated for a specific purpose (the bombing attacks three days before the general Spanish elections);
- The group members performed different tasks, such as planning the attacks, training for the attacks, assembling the explosives and performing the attacks. The division of labor does not imply that every member did only one task during the bombing preparation and execution process. Some members participated in multiple tasks before the Madrid attacks (Haahr-Escolano, 2005);
- The communication among the terrorist members was achieved with the use of cell phones or occurred when they met in specific places (a safe house outside Madrid and a phone shop that was owned by a terrorist). These meetings and communication interactions were vital to the group's decision cycle and to the information-based decision process that was occurring within the specific terrorist network; and
- All of the points mentioned above occurred continuously through time.

Thompson (1967) suggests a typology of three types of interdependence and coordination. When each member of the group performs a task that is not dependent on any other task, and the overall project completion is the sum of the required tasks, then the tasks are pooled interdependent. When, in addition to pooled interdependence, the tasks are performed in sequential order where task B is performed after the completion of task A and task A is not dependent on task B, then the tasks are sequentially interdependent. When, in addition to sequential interdependence, the outputs of each task become the inputs of other tasks, then the tasks are reciprocally interdependent. Different

types of coordination manage each type of interdependence. Pooled interdependence is managed by coordination by standardization, which is the establishment of rules and procedures according to which the members operate. Sequential interdependence is managed by coordination by plan, where a schedule is established for the members' actions. Finally, reciprocal interdependence is managed by coordination by mutual adjustment, where members coordinate based on environmental, individual and group characteristics. With an increase of uncertainty in the environment, members tend to rely on coordination with mutual adjustment.

A terrorist attack appears to be divided in distinct sequential tasks in the abstract (e.g., plan, finance, get the explosives, train, and execute), but closer examination of the work performed by terrorist networks implies that the tasks required to perform an attack are reciprocally interdependent (e.g., the output of planning the attack affects the input of financing the attack and vice versa). This thesis examines the tasks performed before the Madrid terrorist attack, which were reciprocally interdependent.

Thompson (1967) suggests, "Organizations seek to place reciprocally interdependent positions tangent to one another, in a common group which is (a) local and (b) conditionally autonomous." Terrorist groups that exist in different countries worldwide, after 9/11 and the wars in Afghanistan and Iraq, operate autonomously at a local level (Benjamin & Simon, 2005). Therefore, the view of locally autonomous terrorist networks keeps pace with Thompson's proposition.

Thompson (1967) also proposes that '"Organizations with reciprocal interdependence not contained by departmentalization rely on task-force or project groupings to accomplish the remaining coordination." When terrorist networks have members with low levels of experience and different backgrounds (the Madrid terrorist cell) (Wright, 2004) there is not sufficient homogeneity to departmentalize a terrorist attack. Therefore, the networks rely on task forces or project groupings to accomplish the required coordination for a specific project, which, in the Madrid case, was to perform a bombing attack.

According to Galbraith (1977), individuals with low levels of formalization can outperform members with high formalization when they operate under conditions of high uncertainty. Also, experience is a key factor in the group's performance. Highly experienced members produce fewer exceptions and errors than the inexperienced ones in either stable or unstable environments. The Madrid terrorist network had members with low formalization (Benjamin & Simon, 2005). The network did not have distinct jobs for each member, and the members were characterized as "amateurs" since none had participated in any terrorist training camp or had performed terrorist attacks in the past (Haahr-Escolano, 2005). All these theoretical propositions constitute a basis for the Agent Based Modeling manipulations described in the research design in Chapter IV.

D. COMPUTATIONAL ORGANIZATION THEORY

Computational organization theory focuses on computations and simulations of complex organizational models that cannot be analyzed completely with quantitative or qualitative conventional research techniques (Carley & Prietula, 1994). Computational tools are designed to simplify a complex real world problem. If the problem can be simplified without losing any of its key elements, then the tool is of some value. If the problem cannot be simplified appropriately with the available tool, then the results will be inaccurate (Miller & Page, 2007). Hence, research performed with computational tools must be question driven and not tool driven, because not all questions can be answered with all computational tools (Burton & Obel, 1995). In this thesis, POW-ER software was carefully selected since it provides insights about the contingencies that affect the process of performing a terrorist attack based on the Madrid bombing case study.

According to Simon (1996) and Eipstein (1999), computer-based computational models generate virtual environments that imitate actions and behaviors of social life based on real world observations. The model's simplicity is vital in every simulation. Every model must be complex up to the point where no critical attribute or element is excluded from the model (Burton & Obel, 1995). Some details from the real world can be ignored as soon as the main building blocks have been captured by the model (Miller & Page, 2007). Simon (1996) suggests that "we do not have to know, or guess at, all the

internal structure of the system but only that of it that is crucial to the abstraction." Carley and Prietula (1994) do not refute the need for simplicity; however, they emphasize three reasons for adding the necessary complexity to a computational model. The first reason is that the problem may contain nonlinearities that cannot be represented in a different way. Second, some modelers use discrete variables that need to be analyzed with difference equations, and others use continuous variables that need to be analyzed with differential equations. Difference equations increase the realism of organizational simulation models because organizations, people and facts are discrete variables, but decrease the solvability of the model. Researchers should determine the complexity of their models based on the organization under study and the research question they try to answer. Third, agents are adaptive to other agents' behavior; therefore, group behavior is "self-referential". In this thesis, the baseline model of the Madrid terrorist cell, as it is presented in Chapter IV, is an abstraction that captures the key elements of the terrorist network, ignoring any information that is not crucial to the research question.

There are mainly two approaches in computational modeling. The top down approach abstracts general properties from the real world and with the use of feedback loops examines the system's behavior (Epstein & Axtell, 1996). The bottom up approach focuses on the interactions at the lowest level of the system (the individual level) which, by simulation, generates the emerging system behavior (Burton & Obel, 1995). Agent Based Modeling (ABM) is a bottom up approach that examines the system's behavior based on the agents' interactions. Each agent in ABM may follow its own behavior rules, adding complexity and realism to the model. ABM can be generated even if there is ignorance about the general behavior of the system. If the agents' interactions are known, then the general properties of the system emerge with the simulation of these low level interactions (Miller & Page, 2007). Borshchev and Filippov (2004), after taking into consideration various simulation techniques (Agent Based Modeling, System Dynamics, Discrete Events and Dynamic Systems), suggest that, for systems that contain large number of agents, "Agent Based Modeling is more general and powerful because it

enables to capture more complex structures and dynamics." ABM is also powerful for small-scale systems when the overall behavior of the system is unknown but the behaviors at the individual level are known. This is a major reason why ABM was selected for this thesis.

III. THE MADRID ATTACK

This chapter covers the background of the terrorist group that was responsible for the March 11, 2004, Madrid bombings, and the events that occurred from the day of the attack until the capture of the core members of the terrorist cell.

A. THE MADRID TERRORIST CELL

The appearance of terrorist groups in Spain dates back to the early 1980s. On July 20, 1984, the Spanish police arrested an Iranian terrorist, a member of the terrorist group "Martyrs of the Islamic Revolution," who was planning to bomb a Saudi plane in Madrid. That same year, the group "Islamic Jihad" killed citizens with Saudi ties inside Spanish territory; they were accused of bombing a restaurant in Torrejón in 1985. Several years later, the Spanish police captured members of a terrorist group with links to Hezbollah who were transporting a large quantity of explosives through Spain to France (Jordan & Horsburgh, 2005). All the attacks that occurred during the 1980s were performed by individuals, members of Jihadi cells who were neither Spanish residents nor citizens. However, the groups that emerged during the 1990s were composed primarily of Spanish residents. The most important of these groups were the Algerian Jihadi network and the Madrid bombing network. These two groups were not acting independently, since some individuals participated in both networks. This thesis examines the Madrid terrorist network and highlights its connections with other terrorist groups.

After the 9/11 attacks, the Spanish police identified a terrorist cell in Spain that was connected with Al Qaeda. Imad Eddin Barakat Yarkas, aka Abu Dahdah, was believed to be the leader of this cell, which was part of the Algerian Jihadi network. Dahdah was captured in November 2001 (Haahr-Escolano, 2005; Green, 2005). According to the Spanish authorities, his arrest resulted in the disruption of the terrorist cell (Benjamin & Simon, 2005; Green, 2005). According to the Eleventh March (11-M) Commission that was formed after the Madrid attacks in 2004, the Spanish authorities

failed to understand the extent of the Jihadi terrorist network in Spain after the arrest of Dahdah in 2001, and they underestimated the threat of terrorist attacks by Jihadi groups on Spanish soil.

After Dahdah's arrest, the Moroccan Amer Azizi, who had close ties with Dahdah, started recruiting individuals, mainly of Moroccan origin who had some connections with Moroccan extremist groups or shared common beliefs about the "holy war" against the Westerners (Jordan & Horsburgh, 2005). One of the first members to join the group was Sarhane Ben Abdelmajin Fakhet (known also as "The Tunisian"). He was the leader and coordinator of the Madrid bombings (BBC News April 4, 2004; Bennhold, 2004; Wright, 2004), and he had been planning the attack with Rabei Osman el-Sayed Ahmed ("Muhammad the Egyptian") since 2003 (Benjamin & Simon, 2005). Fahket had lived in Spain for eight years, studied economics (Benjamin and Simon, 2005; BBC News, April 5, 2004) at the Autonomous University of Madrid (Bennhold, 2004) and also worked as a real estate agent (Wright, 2004).

Muhammad the Egyptian was referred as the Architect of the attacks. He was an expert in bombs due to his service in the Egyptian Army as a specialist in explosives (BBC News, March 10, 2005; Wright, 2004); he was the only member of the terrorist cell with such expertise. Despite his previous military experience, he had not previously joined any Al Qaeda training camps or fought for the Jihad abroad. A conversation between him and another terrorist on the cell phone some days after the attacks was recorded; in this recording, he clearly stated that the Madrid bombings were his project. "I was ready to blow myself up, but they stopped me, and we obey God's will," he said. "I had wanted a heavy burden, but I didn't find the means. This plan cost me a lot of study and patience. It took me two and a half years" (Sciolino & Horowitz, 2004).

Jamal Ahmidan, Fakhet's right hand man, was a Moroccan who was the cell commander of the terrorist group (BBC News, April 4, 2004; BBC News, April 5, 2004; Benjamin & Simon, 2005; Wright, 2004) and was involved in small drug smuggling (Jordan & Wesley, 2006) with the Oulad Brothers and Abdennabi Kounjaa (Benjamin & Simon, 2005; Wright, 2004). Ahmidan was also the cell recruiter: he had recruited Moroccans such as Kounjaa and the Oulad brothers, who had no prior terrorist

experience. Ahmidan did not plant any bombs on the day of the attack, but he rented a farmhouse outside Madrid where the bombs probably were assembled. His connections with criminals provided the group the necessary links to the bomb providers. Ahmidan exchanged drugs for explosives with a drug dealer, Jose Emilio Suarez Trashorras, who had friends who were miners and could steal some explosives from their workplace (Benjamin & Simon, 2005). Ahmidan received 200 kg of Goma-2 explosives and transported them to the rented farmhouse.

The members of the terrorist group assembled the bombs by connecting the explosives with cell phones and detonators and placing them inside large handbags. What remains unknown is how the members of the group acquired the knowledge to build the bombs. They may have gathered this information through manuals or other sources found on internet sites, since the internet has become a virtual training camp for terrorist cells (Wiemann, 2006). Evidence supporting this view has not been found yet; therefore, this thesis assumes that the knowledge and the guidance for the bomb building process was provided by Rabei Osman el-Sayed Ahmed (Muhammad the Egyptian or The Architect), since he was the only member of the group who was an expert in bombs (Wright, 2004).

Before the attacks, many of the members of the Madrid terrorist network were captured by the police for other crimes (e.g., drug smuggling) at different times, but they never were connected to any terrorist group. The Spanish authorities' false belief that the terrorist network in Spain was neutralized after Abu Dahda's arrest in 2001 resulted in the lack of correlation between terrorism activities and drug smuggling crimes. If that correlation had occurred earlier, the terrorist cell could have been delayed or even disrupted since it would not have had the funds to perform a bombing attack (Haahr-Escolano, 2005).

The Madrid terrorist group did not have any financial relations with any Al Qaeda operatives. The group was self-funded, and most of its resources came from drug smuggling activities (Benjamin & Simon, 2005; Wright, 2004). For the jihadists, outlaw activity is acceptable only when it is carried out for the sake of the Jihad (Haahr-

Escolano, 2005). The whole operation's cost was about $50,000, which is a very small amount considering the level of casualties and the effects the bombings had on Spain's policy regarding its troops in Iraq (Benjamin & Simon, 2005).

B. THE 2004 MADRID BOMBINGS

On March 11, 2004, one of the largest terrorist attacks in the history of Spain occurred, causing the deaths of 191 people and wounding 1800 more (Jordan & Wesley, 2006). The purpose of the attack, consistent with the fact that it occurred three days before the general elections, was to pressure the Spanish government to withdraw its troops from Iraq (Haahr-Escolano, 2005; Benjamin & Simon, 2005). The terrorists viewed the attacks as a message to the other countries that had troops in Iraq to either withdraw them or live under the fear of a similar attack on their own soil (Wright, 2004).

The attacks occurred on four trains: three originating from Alcala de Henares (a village 18 miles northeast of Madrid) and one from Guadalajára. The first train departed from Alcala de Henares at 0604 GMT, and the other two left fifteen minutes apart (BBC News, April 4, 2004; Benjamin & Simon, 2005). At 0639 GMT, when the first train reached the Atocha station, three bombs exploded in three different wagons of the train. At the same time, another three bombs detonated on the second train, which was two minutes delayed, 500 yards from Atocha station. Ninety-three people were killed and hundreds were wounded in these two attacks (Benjamin & Simon, 2005). Two minutes later, two bombs detonated on the third train that had departed from Alcala de Henares. This attack occurred at the El Pozo station, which was the previous station on the train route before the Atocha station. This attack killed 70 people and wounded many more. If the train had not been delayed, there probably would have been more innocent victims, since a quarter million passengers pass through the Atocha station every day (Wright, 2004). One minute later, a bomb exploded on the fourth train while it was passing through the Santa Eugenia station two stations away from the Atocha station (Benjamin & Simon, 2005).

All Spanish emergency services rushed to the bombing scenes to provide help to wounded citizens (BBC News, April 4, 2004). While the emergency rescuers were searching the train wreckage for survivors, they frequently came across various passengers' belongings, which they delivered to the local police station after their sector search was over.

Hours after the attack, the Popular Party Prime minister José Mariá Aznar declared that the Basque terrorist group Euskadi Ta Askatasuna (ETA) was responsible for the attacks, since they occurred three days before the general elections, and ETA had performed bombings on trains in the past (Haahr-Escolano, 2005; Benjamin & Simon, 2005; Wright, 2004). According to members of the Popular Party, ETA wanted to bring chaos to the elections. However, early findings indicated that the methods used in the attacks were not similar to the methods used by the Basque terrorist group in the past. ETA's attacks always came with a warning, and their targets were not innocent civilians, since this would have a negative impact on ETA's popularity among the Spaniards (Wright, 2004).

After the 9/11 attacks, a rental car that had flight manuals in Arabic was found near Boston's airport. Based on this knowledge, the authorities immediately investigated a report about an abandoned Renault Kangoo outside Alcala de Henares station. Inside the van, the police found seven detonators and a tape with verses from the Koran in Arabic. This clue was a clear indication that Islamic extremists may have been responsible for the train attacks that had occurred earlier that day (Benjamin & Simon, 2005).

Twelve hours after the attack, a cell phone rang inside a bag that was found at the El Pozo station. The police opened the bag and, to their surprise, found that the cell phone was attached to two detonators that were connected to explosives. The bag also contained screws and nails in order to cause more deaths once it exploded. This was clearly a bomb that had failed to detonate. The police examined the SIM card that was inside the phone and obtained evidence that led to the arrest of five suspects: three Moroccans and three of Indian origin (BBC News, April 4, 2004; Benjamin & Simon, 2005). The Spanish authorities interrogated the suspects and found connections with the

terrorist group that had performed similar attacks in Casablanca the previous May, killing forty-one civilians (BBC News, May 17, 2003). This Moroccan group had close ties with Al Qaeda, and the Spanish authorities were almost convinced that ETA had not performed the terrorist attack.

The final confirmation that Jihadi groups were behind the attack came from a videotaped message in Arabic that was received on March 13, 2004, in which a man declared responsibility for the attacks. In the message he clearly said, “We declare our responsibility for what happened in Madrid ... It is a response to your collaboration with the criminals Bush and his allies ... There will be more if God wills it. You love life and we love death ... if you don't put an end to your injustices more and more blood will run.” (Wright, 2004)

The terrorist cell did not use all of the explosives it had in its possession for the March 11, 2004, attacks. Bombs similar to those that were used for the March 11 attacks were found on the Madrid-Seville speed train on April 2, which indicated that the terrorists were planning to perform more attacks, but an unknown and unexpected event on April 2 ruined their plans (Benjamin & Simon, 2005; Wright, 2004).

On April 3, 2004, the police had indications that the terrorists were in an apartment in a suburb of Leganes, an area south of Madrid. A police force surrounded the building and asked the terrorists to surrender. Instead, the terrorists blew themselves up, wounding a police officer in the process. The leader, the cell commander and five members of the terrorist cell were among the dead terrorists (BBC News, April 4, 2004; Bennhold, 2004).

IV. RESEARCH DESIGN

This chapter initially covers the research method and frames the Baseline model, which is an abstraction based on real world data from academic papers and news articles about the terrorist cell that performed the 2004 Madrid attack. The research design then describes the Expert and the Hierarchical models, and the manipulations made for each model that was created based on the baseline model. In design terms, this chapter suggests a 3 x 2 factorial design with three different representations of a specific terrorist group (i.e., the Baseline, the Expert and the Hierarchical models), under two different mission-environmental contexts (i.e., Baseline and high counterterrorist conditions).

A. RESEARCH METHOD

Virtual Design Team (VDT) models are Agent Based Models, and the VDT program has been developing continuously accumulating research for more than two decades, building organizational models based on real world cases in order to examine their underlying organizational processes (Levitt et al., 1999). VDT modeling is based on an information processing view of organizations developed by Galbraith (1977), Simon (1976), and March and Simon (1958). According to Galbraith (1977), organizations are information processing systems that have a specific communication and information exchange infrastructure in which lower level information processors (individuals or teams) have predefined roles and accomplish specific tasks. These individuals or teams send information through some formal lines of communication and information exchange (e.g., telephone lines and mails) that, depending on the way they are organized (e.g., as Machine Bureaucracy or Adhocracy (Mintzberg, 1980)) and the sequence of the tasks that have to be completed, affect overall organizational performance. The actors' information capacity is limited following the model of "bounded rationality" proposed by Simon (1976). Hence, the VDT models can predict the performance of alternative organizational configurations that perform a specific task (Carley & Prietula, 1994).

The VDT models are agent-based representations, exploring the organization's aggregative behaviors using the bottom up approach. So, by simulating the micro-level organizational behaviors (individual actors or groups), the researcher can use simulation to explore the aggregative effects on the macro-organizational level (Levitt et al., 1999). Figure 1 illustrates the information processing view of the work accomplished by an actor who is part of an organization and performs specific tasks while communicating with the other members. The actor's "In Tray" represents the inputs that are provided to the actor. These inputs can be the direct work that has to be performed for some tasks, meetings to attend, or even communications requests from other actors. The actor performs each task sequentially; therefore, he proceeds to the next task after the previous one has been completed. The "Out Tray" represents the outcomes that emerge from a specific actor. These outcomes can be the completion of a specific task, attendance at a meeting, or communication with another actor. The way an actor manages his inputs in order to generate the outcomes depends on his acquired skill level, the existing backlog, and the number of communications that are received from other actors. The actor's outcome will vary, depending on how much the actor's skill matches the skill required for a specific activity. Of course, as was mentioned before, the work backlog and the number of communications from other actors can affect the outcome since these tasks divert the actor's attention.

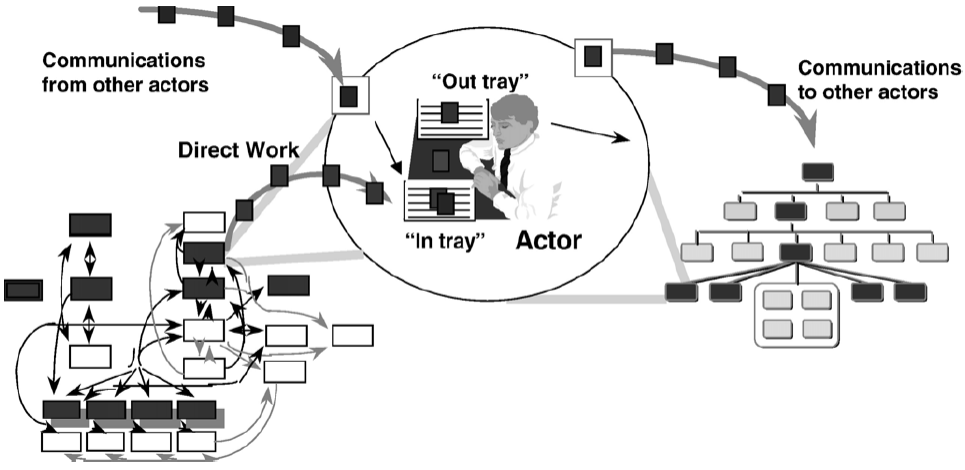

Figure 1. The view of organization structure with the actors and the tasks (After: Nissen & Levitt, 2004)

The VDT modeling program has been extensively validated over the years by using fieldwork data in order to create the simulation models that represent the organizations under examination. Studies in various fields of industry, such as power plant construction (Christiansen, 1993), aerospace (Thompsen, 1998), software development (Nogueira, 2000) and healthcare (Cheng & Levitt, 2001), have been conducted with the use of VDT simulation, emphasizing its applicability in the real world. The models are created with the use of information possessed by the organization at the starting point of the period under examination. Then the generated behavior from the simulation is compared with the actual real world data and is provided to the researchers by the organization's managers. If the computational results are similar to the real world data, then the model can be characterized as a "good" abstraction of reality and can be used for further analysis. This process is called "backcasting," and it is a docking technique used by the VDT in order to validate the generated models (Kunz et al., 1998). Backcasting has been used extensively by researchers (Christiansen, 1993; Thompsen, 1998; Cheng and Levitt, 2001). This thesis examines the March 11, 2004 Madrid bombings by using the method of "backcasting" in order to develop the baseline model. This thesis follows all the stages of "backcasting" except from the last comparison stage; data could not be provided by the terrorists since most of them are dead and the living are hard to reach. The studies that have been performed analyzing the terrorist network that is responsible for the 2004 Madrid bombings (Jordan and Horsburgh, 2005; Rodriguez, 2008) are used instead.

In order to summarize the VDT modeling structure and emphasize the value of the knowledge created with the use of this computer simulation, it is useful to represent VDT as an Inquiring System (Mitroff & Murray, 1993; Mitroff, 1995). Figure 2 illustrates Mitroff's Inquiring System. Inquiring Systems are systems that create "new knowledge" based on some process, given certain inputs. The main components of an Inquiring System are the inputs, the process that receives the inputs and generates new knowledge, the outputs or the new created knowledge, and the guarantors for the inputs and the process.

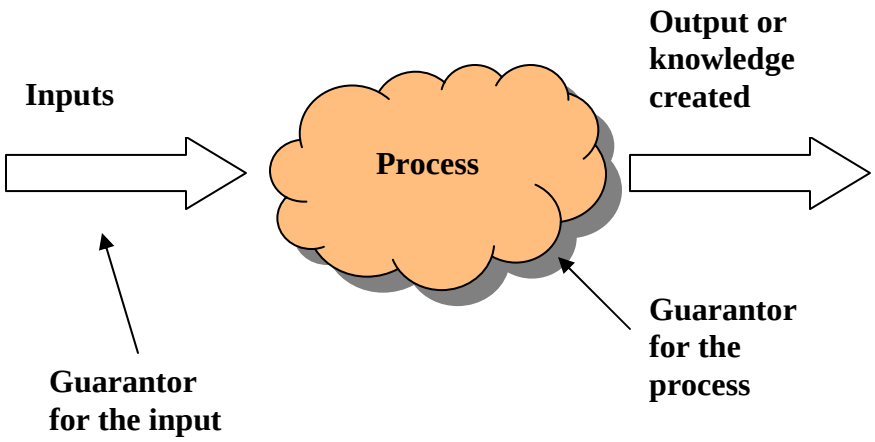

Figure 2. Mitroff's Inquiring System

The inputs for the VDT model are the organizational structure, the activities performed by the members of the organization, the process description of the project under examination, the actors and the communication lines among them (including coordination and rework links) (Kunz et al., 1998). In this thesis, the inputs are provided after extensive research through academic papers and articles that describe or analyze the Madrid bombing attacks. Hence, the guarantors for the inputs are the cross-validated real world data that provide information for the specific case study. The process is the VDT simulation model and the guarantor for the process, as mentioned above, is the research conducted with the VDT simulation for over two decades in various industries that provides external validity to the simulation software. The output of VDT comprises quantitative measures of the required coordination, rework, total work, and others, including the various kinds of risks (communication, functional and project risk), required for project completion. These measures indicate how the inputs affect the outcome and provide useful insights about the effect of different contingency factors on project completion. In this thesis, the outcome also proposes counterterrorist policies that could be adapted to thwart terrorist networks.

B. THE BASELINE MODEL

The POW-ER Agent Based Modeling application used in this research is version 3.5b, and represents a continuation of development (see Nissen and Levitt 2004; Looney and Nissen, 2006; Nissen, 2005a; Nissen, 2005b) that has its roots in the VDT research program. Any bugs or errors that may be inherent in POW-ER 3.5b are controlled and applied consistently across all models. Hence, even though some results may have some errors, these errors apply to all models, leaving unaffected the relative comparison that is of essence in this thesis.

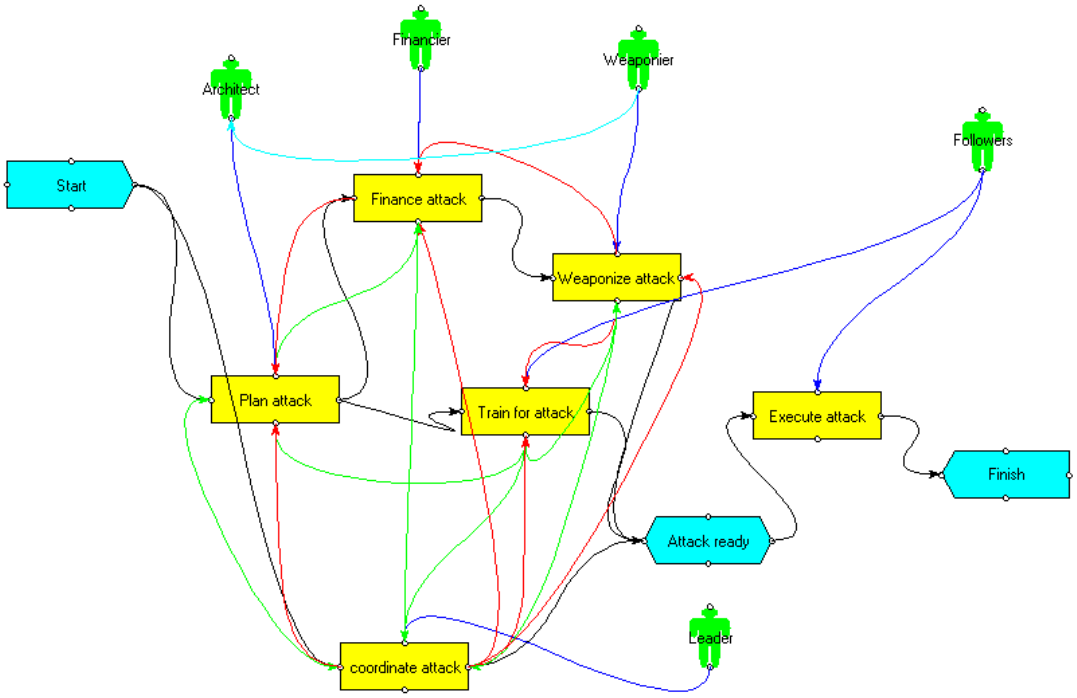

Figure 3. Madrid Cell Baseline Model

Figure 3 illustrates the baseline model of the terrorist network that performed the 2004 Madrid terrorist bombings. Behind each object in the baseline model, either an actor or a task, are a number of model parameters that are set to describe the nature and the key attributes that create the overall behavior of the system. Most of these parameters are set

to “normal” levels based on organizations that have been examined in the past (Jin & Levitt, 1996; Levitt et al., 1999; Nissen & Levitt, 2004; Nissen & Leweling, 2007). The structure of the Madrid network was decentralized and could be characterized as an Edge-like structure (Alberts & Hayes, 2003). The Edge (Alberts & Hayes, 2003) is an organizational archetype with particular applicability in the C2 domain (see Nissen, 2005a, Orr & Nissen, 2006). The Edge shares similarities with the Adhocracy (e.g., coordination by mutual adjustment, small unit size, many liaison links throughout, selective decentralization), Professional Bureaucracy (e.g., low vertical specialization, high training and indoctrination, market and functional grouping), and Simple Structure (e.g., low horizontal specialization, low formalization). The Edge organization also demonstrates several key differences, and it does not correspond cleanly with any single archetype. Key to Edge characterization are decentralization, empowerment, shared awareness and freely flowing knowledge, which are required to push power for informed decision making and competent action to the “edges” of organizations (Alberts & Hayes, 2003), where they interact directly with their environments and other players in the corresponding organizational field (Scott, 2001). Therefore, some general parameters (e.g., noise and communications probability) were set to “normal” levels based on previous research about terrorist groups with Edge and Hierarchical structure, that was conducted with the use of POW-ER software at a theoretical level (Nissen & Leweling, 2007). The model has a start and a finish point (on the far left and right of the figure). Each run begins at the start point and ends when it reaches the finish point. Using a Monte Carlo approach, each scenario is run 100 times.

The actors of the terrorist group (human figures) represent either an individual or a group of people. The actors’ names are mentioned based on their roles. A representation of the actors with their real names based on the Madrid case study was avoided: it is out of the scope of this thesis since the focus is not on the individuals themselves. On the other hand, each actor has the attributes of the participant or the group that participated in the Madrid terrorist network. For example, Fakhet, who was the leader and coordinator of the cell, is represented as an individual who has a team-leading role. The financers are a group of four individuals composed of Jamal Ahmidal, the Oulad Brothers and

Abdennabi Kounjaa (BBC News, March 10, 2005; Benjamin and Simon, 2005). The baseline model's network is compared with existing Social Network Analysis networks that have examined the 2004 Madrid terrorist network. Even though the representation is different and the analysis is made with a completely different method, as described in Chapter II, the SNA networks and the baseline model network have the same number of core participants, and the description of each member is identical (Jordan and Horsburgh, 2005; Rodriguez, 2008). Hence, the empirical representation of the actors and their attributes used in the baseline model are consistent with the existing data from SNA academic papers.

The boxes that are directly connected with the actors represent the tasks performed by the actors. The tasks are sequentially interconnected, some in series and some in parallel. Initially, the attack is planned by the architect and the leader, and afterwards the tasks are performed in three parallel branches that have the same amount of total work. The top branch is composed of the finance and weaponize (buy and assemble the explosives) tasks. At the same time, team members train for the attack, meaning that they identify targets and check the train routes; this forms the second branch. During the same period, the leader has a coordinating role overseeing the progress of the plan, which forms the third branch. When the attack is ready (represented by the milestone "attack ready"), team members execute the attack. The time periods needed for the completion of each task were impossible to select with accuracy, since most of the members of the cell committed suicide approximately one month after the attacks (BBC News, April 4, 2004). According to Benjamin & Simon (2005), Sahrane, who was the coordinator of the attack, stopped showing up for work by the fall of 2003. Moreover, on October 19, 2003, bin Laden released two videotapes in which he prompted Jihadi groups for an attack against the countries that participated in the war in Iraq, such as Spain, Poland, Italy and Japan. A Spanish official suggested that the cell started the planning of the attack the day after the messages' release (Benjamin & Simon, 2005). Therefore, the total "project's" time was set to four months in our models. The coordinator was performing his task during the whole four month period, except during the execution phase; Sahrane (the coordinator) stayed at the farmhouse (the place where

the terrorist met and assembled the bombs) the day of the attack and was not part of the "execution phase group." In addition, the terrorists acquired the explosives in January 2004 (Benjamin & Simon, 2005) and had only the next month (February 2004) to assemble them. Therefore, the finance and weaponize task was set to one month each. Hence, the first two months were devoted to planning. The analysis of the network is performed comparatively; therefore, errors that may exist in the model's task durations do not influence the outcome of this thesis.

Parameter	Baseline Model Values
Application Experience	Low
Skill Level	Low
Task Uncertainty	Medium
Task Complexity	Medium
Rework Strength	0.10
Centralization	Low
Formalization	Low
Team Experience	Low
Matrix Strength	High
Communication Probability	0.60
Noise Probability	0.20
Functional Exception Probability	0.15
Project Exception Probability	0.15
Organizational Levels	1

Table 1. The Main Parameters of the Baseline Model

The key parameters of the baseline model are summarized in Table 1. According to Galbraith's view of organizations as information processing systems, exceptions are situations in which an actor does not have the required information to accomplish a task, which normally requires him or her to go to a higher level in the hierarchy or to a knowledgeable person in order to handle the created exceptions. However, an exception may be handled or ignored. If it is ignored, it causes a decrease in the project's (e.g., the terrorist attack) quality. Each task requires a skill that needs to be matched with the actor's skill in order to generate as few exceptions as possible. Therefore, if an actor who performs a task has a high level of a specific skill that is required for the task (for

example, an expert on weapons is performing the “weaponize” task), then the task will be performed with few exceptions. Application experience, on the other hand, is the level of experience the actor has on the assigned task.

The main distinction between application experience and skill level is that an actor may have a high level skill that matches the skill required for task completion, but have no prior experience with the execution of the specific task. In the Madrid terrorist cell, the financers had no prior experience with financing a terrorist act, so their application experience is set to low. In general, the design and the execution of the 2004 Madrid terrorist attacks were not done by Al Qaeda operatives (Benjamin and Simon, 2005). The Madrid terrorist cell had individuals who were Spanish residents, shared common ideas and beliefs about jihad among themselves and with Al Qaeda, but did not formally belong to the “Al Qaeda organization” (Haahr-Escolano, 2005). None of the members of the Madrid terrorist cell had been trained in any of Al Qaeda’s training camps in Bosnia, Afghanistan and elsewhere (Benjamin & Simon, 2005). The network was composed of “amateurs,” since the members of the terrorist cell had neither previous experience nor training to conduct terrorist acts (Jordan & Wesley, 2006). For this reason, the Application Experience in the baseline model was set to low for all members. The required skill levels for all actors were also set to low for the reasons mentioned above, except for the Architect (Muhammad the Egyptian), who was an expert in bombs and therefore had a high “weaponize” skill.

Since the Architect was the only member of the group who had knowledge about bombs, the model has a knowledge link that starts from the actors who assemble the bombs and ends at the Architect. This knowledge link indicates the path that actors who encounter exceptions should follow in order to reach the appropriate actor who can manage the exceptions that are generated during the execution of the actors’ task.

The level of task uncertainty indicates the amount of information that the actor is missing as he goes about completing a task, and task complexity represents the relative difficulty of performing a specific task. For the Madrid case study, the levels of uncertainty and complexity are set to medium since there are no indicators to justify a change of these values for the specific attack.

The coordination links (green lines among tasks) indicate that, in order to complete a specific task, actors have to communicate with other actors. For example, the team that is responsible for the bombs communicates with those who train for the attack and vice versa. The rework links (red lines), on the other hand, are unidirectional. An exception created at a specific task might generate rework for another task. For example, an exception created during the financing task might create rework at the planning task, since new parameters must be taken into account for the successful planning of the operation. Each rework link has an embedded value that characterizes the rework strength. Rework strength of 0.1 implies that 1 day of rework in the source task will cause 0.1 day of rework in the target task.

The level of centralization indicates which organizational level has the decision-making responsibility within the organization. A low level of centralization suggests that all expect decision rights remain at the lowest levels of the organization. Similarly, a high centralization level indicates that all decisions are made at the highest levels of the organization. The centralization of the Madrid terrorist network is set to low because, even though the network had a leader and an architect, all decisions were made by the actors at the lowest level of the organization. The Madrid terrorist cell was a decentralized network that acted as a group focused on the completion of its project, the terrorist attack.

Formalization, according to Organization Theory, is based on the degree to which work structures and job descriptions are rigidly defined within the organization. The formalization of the network is set to low because the members of the network did not have predesigned tasks and their jobs were not predetermined from the planning phase of the attack. The available open source data (academic papers and news articles) provide the opportunity to separate the network's activities into explicit subtasks.

Team experience is the experience the team has on the specific type of project. Even though all the members of the terrorist group had the same beliefs, shared the same ideas and had friendship or family ties, they had never performed a terrorist attack together. Therefore, their team experience is set to low. Matrix strength indicates the

tendency actors have toward coordination among horizontal lines. In the Madrid terrorist cell, members relied completely on lateral relations; therefore, the matrix strength is set to high.

The communication probability of 0.6 indicates that 60% of the total amount of communications are successfully performed among actors. According to Kunz, et al. (1998), noise consumes actors' time without contributing to performance. Therefore, a noise probability of 0.2 indicates that 20% of the actors' total time is spent on things that are not related to the project. The parameters Functional Error Probability (FEP) and Project Error Probability (PEP) address two different aspects of environmental difficulty. FEP indicates the probability of organizations making errors and causing exceptions at the functional level, and PEP indicates the probability of organizations making errors and causing exceptions across functions that affect the whole project.

The organizational levels indicate the vertical levels that exist within the organization. For example, Edge has one organizational level, Simple Structure and Professional Bureaucracy have two, and Machine Bureaucracy has three or more organizational levels. The values of rework strength, communication probability, noise probability, FEP and PEP presented in Table 1 are patterned in particular after relevant, previous work (Gateau et al., 2007; Nissen & Leweling, 2007) and the interested reader is directed to this previous work for more details.

C. THE EXPERT AND HIERARCHY MODELS

Even though the Baseline model does not capture the relations among the individual members of the group, such as family, occupational or friendship relations, it provides the opportunity to examine the structure and the workflows of the terrorist network that was responsible for the 2004 Madrid bombings. It allows us to develop variations of this model in order to answer the research question and generate suggestions about ways to thwart terrorist groups. Table 2 summarizes the variations of the Baseline model.

Parameter	Baseline Model Values	"Expert" Model Values	"Hierarchy" Model Values
Skill levels	Low	High	Medium
Application Experience	Low	High	Low
Team Experience	Low	High	Medium
Formalization	Low	Low	High
Centralization	Low	Low	High
Matrix Strength	High	High	Medium
Communication Probability	0.60	0.60	0.30
Noise Probability	0.20	0.20	0.10
Functional Exception Probability	0.15	0.15	0.05
Project Exception Probability	0.15	0.15	0.05
Organizational Levels	1	1	3

Table 2. Model Manipulation Variables

The 2004 Madrid terrorist cell was composed of "amateurs" (Haahr-Escolano, 2005) with low skill and application experience levels. The threat of amateur terrorists is examined in comparison with an "expert model" that substitutes experts for amateurs. The "experts" in the expert model have high skill levels that match the tasks' required skills; for example, an expert on weapons is performing the "weaponize" task. Their application experience also is high, which indicates that they have performed the tasks repeatedly in the past. The team experience is set to high, indicating that the expert group had performed these terrorist tasks in the past as a team. All other model parameters are the same as in the Baseline case.

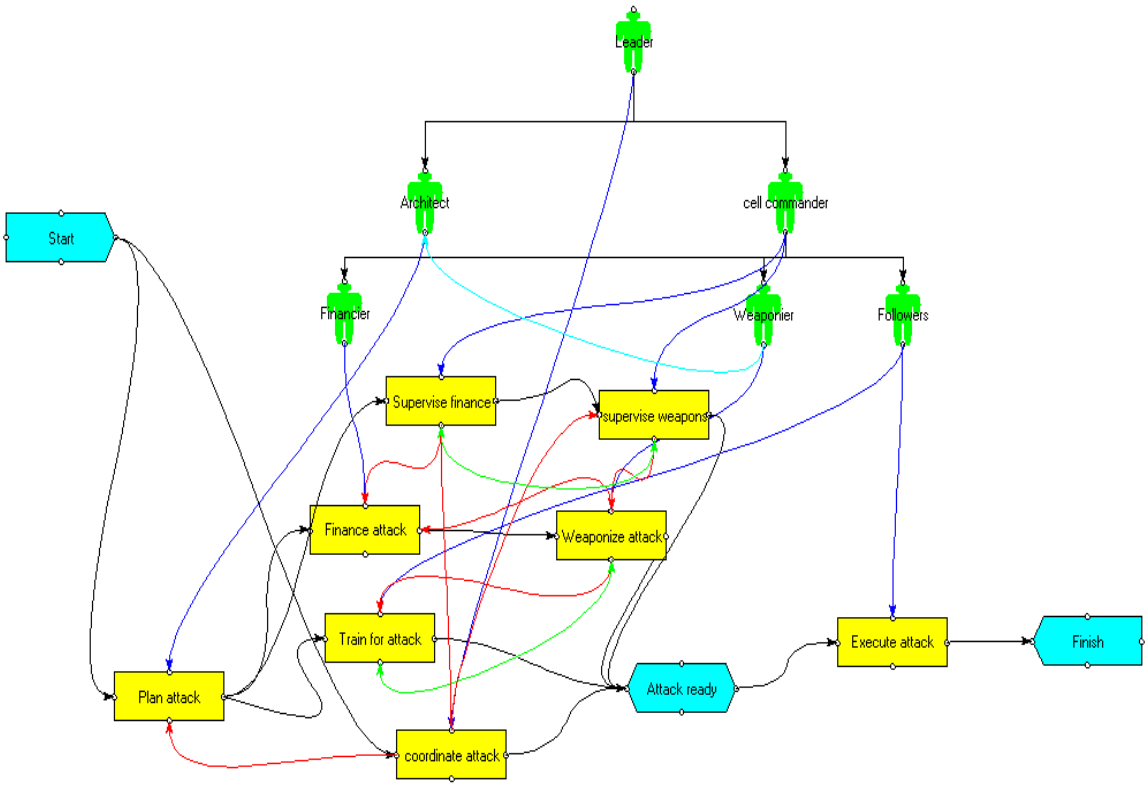

Figure 4. Madrid Cell Hierarchy Model

Despite the fact that many terrorist networks are decentralized and are not branches of the AQ organization, some appear to be locally organized as a hierarchy. Therefore, a hierarchical model is introduced, where the structure of the network is a three-level hierarchy. Figure 4 illustrates the Hierarchical model of the Madrid terrorist cell. The key attributes of both the actors and the tasks are the same as the baseline model. The total work performed in both the Baseline and the Hierarchical model is identical. The leader stands at the top of the hierarchy; the architect and the cell commander are the terrorist organization's middle managers. The financers, weaponiers and followers operate at the lowest level of the organization and are subordinates of the cell commander. The values of the parameters presented in Table 2 for the Hierarchical structure are patterned after previous POW-ER models that characterized organizational hierarchies (esp. Looney & Nissen, 2006; Gateau et al., 2007).

D. THE COUNTERTERRORIST CONDITIONS

The three models introduced above are tested under different "counterterrorist conditions." In general, counterterrorist actions may lead to the destruction of a terrorist cell or to the arrest of terrorists that prepare a terrorist attack. This thesis examines the Madrid terrorist network, which was a "successful terrorist project", where no member was captured before the execution of the attack. Therefore, in this thesis counterterrorism conditions are composed of three basic elements. The first is the noise probability, the second is the level of task uncertainty, and the third is the level of task complexity. The values of these parameters for the Baseline case were analyzed earlier in the chapter.

	Baseline Counterterrorist Conditions	**High Counterterrorist Conditions**
Noise	0.20 or 0.10 (Hierarchy)	0.80 or 0.40 (Hierarchy)
Task uncertainty	Medium	High
Task complexity	Medium	High

Table 3. Baseline and High Counterterrorist Conditions

High counterterrorist conditions occur when counterterrorist agencies perform a high level of counterterrorist acts in order to distract terrorist members from their prior tasks. Therefore, the noise probability is greater for high counterterrorist conditions. According to Sterman (2000), extreme input values give the opportunity to the researcher to observe with greater clarity and confidence the differences that occur at the outputs. Therefore, the noise probability value for the high counterterrorist conditions is set four times greater than the noise probability of the Baseline case. High counterterrorist conditions also imply that the terrorists will perform their tasks with greater uncertainty (have less information to complete the task) and the task itself will become more difficult (high task complexity). This manipulation aims to explore the effect that intense counterterrorist acts have on terrorist networks while they are planning to execute a terrorist act. Table 3 summarizes the differentiating variables under the two counterterrorist conditions.

	Baseline Model (Low Expertise)	Expert Model	Hierarchical Model
Baseline Counterterrorist Conditions			
High Counterterrorist Conditions			

Table 4. The 3 x 2 factorial research design

To summarize, this thesis examines three different terrorist organizations under two different counterterrorist conditions, in order to provide insights about the network's underlying structure. In design terms, it is a 3 x 2 factorial design with three different representations of a specific terrorist group (i.e., the Baseline, the Expert and the Hierarchical model), under two different mission-environmental contexts (i.e., Baseline and High counterterrorist conditions). The results of these comparisons are presented analytically in Chapter V.

THIS PAGE INTENTIONALLY LEFT BLANK

V. RESULTS

This chapter examines the simulation results of the various model manipulations presented in Chapter IV. Initially, a comparison is made between the Baseline model, which is composed of low skilled and inexperienced members, and the Expert model (EX), which is a representation of the baseline model with highly skilled and experienced members. Then the Baseline model is compared with the Hierarchical model. All comparisons presented are also tested under two different environmental conditions, the baseline (BCC) and high counterterrorist (HCC) conditions, in order to examine how different environmental conditions affect the models mentioned above. Finally, all models are compared holistically under the two different environmental conditions.

The simulation results for all models are summarized in Table 5. We first compare the Baseline, the Expert and the Hierarchical model under baseline counterterrorist conditions then compare the same models under high counterterrorist conditions. The differentiations of the models' variables are described in detail in Chapter IV. The values in bold of Table 5 indicate the lowest value for each variable in the two different counterterrorist conditions.

	Baseline Counterterrorist Conditions (BCC)			High Counterterrorist Conditions (HCC)		
Scenarios / **Parameters**	**Baseline**	**Expert (EX)**	**Hierarchy**	**Baseline**	**Expert (EX)**	**Hierarchy**
Duration (days)	*404*	***197***	*425*	*408*	***198***	*458*
Rework (person-days)	***65***	*94*	*82*	***69***	*96*	*102*
Coordination (person-days)	*222*	*256*	***42***	*255*	*317*	***68***
Wait Time (person-days)	*26*	***4***	*61*	*23*	***3***	*84*
Communication Risk (probability)	*0.61*	***0.55***	*0.60*	*0.61*	***0.56***	***0.56***
Functional Risk (probability)	*0.75*	***0.20***	*0.75*	*0.75*	***0.20***	*0.73*
Project Risk (probability)	*0.71*	*0.71*	***0.56***	*0.72*	*0.71*	***0.55***

Table 5. Simulation Performance Results

A. BASELINE COUNTERTERRORIST CONDITIONS' MODEL COMPARISON

Beginning with the results of the Baseline model under Baseline Counterterrorist Conditions (BCC), that are reported in the second column of Table 5, the terrorist organization accomplishes its tasks in 404 days; this is a measure of organizational speed which is very important for performing a terrorist attack under time constraints. (The 2004 Madrid attack had to be performed some days before the Spanish general elections in order to create a greater impact (Wright 2004)).

For reference, although the exact duration of this "terrorist project" remains unknown, certain informed estimates vary from four months (a Spanish official suggested that the cell started the planning of the attack the day after the release of bin Laden's messages at the end of October 2003 encouraging terrorists to attack Spain (Benjamin & Simon, 2005)) to thirty months (a terrorist claimed, "This plan cost me a lot of study and patience. It took me two and a half years" (Sciolino & Horowitz, 2004)). The simulation result of 404 days (i.e., roughly 14 months) is close to the mean of these estimates.

Continuing with Baseline results in the table, the level of rework (65 person-days) reflects the level of effort expended attending to exceptions and correcting errors that are made during the "terrorist project." Coordination (222 person-days) reflects the level of effort expended for coordination between the various actors of the terrorist network. The 26 person-days of wait time reflect the amount of time that actors spent waiting for decisions to be made and information to be provided.

The communication risk of 0.61 indicates that 61% of the total communications' volume that occurs among actors is likely to be ignored or addressed inadequately. Functional risk of 0.75 indicates that, on average, 75% of the exceptions that are created for a particular functional area (for example the planning task) are inadequately reworked or ignored by the actors. Finally, project risk of 0.71 indicates that, on average, 71% of the exceptions that are created across functional areas are ignored or inadequately resolved by the actors of the organization. According to Ramsey and Levitt (2005), project exceptions are related to the interface issues of the functional and knowledge areas of the project.

For comparison, the Expert model requires only 197 days to accomplish the terrorist tasks. This is less than half of the time duration required in the Baseline model; therefore, the expert organization moves much faster than the Baseline. The Expert model also involves more rework (94 person-days). This is almost 50% more in comparison with the Baseline model and indicates that a greater number of exceptions and errors are corrected by the Expert organization. Coordination (256 person-days) is greater for the Expert organization also, since the organization's actors need to coordinate more in order to rework more exceptions. Wait time in the Expert organization is 4; this is almost one sixth of the wait time for the Baseline organization. This occurs because actors that are connected with knowledge links in the expert organization do not have to wait long for experts to provide them with information, since they are experts themselves and the exceptions that are handled through the knowledge links are few.

The communication risk is lower for the Expert organization (0.55) since the team experience is high in comparison to the low team experience of the Baseline organization. The large number of reworked exceptions also is reflected in the functional risk of the

Expert organization (0.20) which is almost one quarter of Baseline's functional risk. Finally, project risk level (0.71) is approximately the same as the Baseline organization. Hence, even though the Expert model entails almost the same risk as the Baseline organization, it is faster than the Baseline model.

For comparison with the Baseline, the Hierarchy requires roughly 21 days more time to accomplish its terrorist attack tasks and hence moves somewhat more slowly. This is consistent with results in other contexts (e.g., joint task force, see Gateau et al., 2007; coalition mission planning, see Looney and Nissen, 2006; Computer Network Defense, see Koons et al., 2008). In comparison to both the Baseline and the Expert models, the Hierarchy is the slowest of all. The Hierarchy involves a greater level of rework (82 person-days) in comparison to the Baseline model, which indicates that a greater number of exceptions and errors are corrected by the Hierarchical organization than the ones reworked by the Baseline organization. On the other hand, the Hierarchy requires less rework in comparison to the Expert model. Coordination (42 person-days) is considerably less for the Hierarchy than for either the Baseline or Expert models, as actors without a hierarchical organization are required to coordinate abundantly and laterally. However, wait time (61 person-days) is almost two and a half times greater in comparison to the Baseline and fifteen times more in comparison to the Expert model, as actors in the Baseline and the Expert models do not have to wait for supervisors to make decisions or provide information.

The communication and functional risks are comparable for both the Baseline and Hierarchy (0.61 vs. 0.60), indicating the immunity of these variables to structural change. As with the Baseline, however, the functional risk of the Hierarchy (0.75) is much greater in comparison to the Expert model (0.20), since more exceptions are reworked in the Expert model. Finally, project risk level (0.56) is appreciably lower for the Hierarchy. Hence, the Hierarchy entails less project risk in comparison to the other two models (Baseline and Expert models).

Therefore, there is a set of strengths and weaknesses that characterize these models under BCC; these are summarized here. First, the Baseline model requires the least rework in comparison with the other two models. Moreover, the Baseline model is

faster and requires less wait time in comparison with the Hierarchical model. The Baseline model also requires less coordination in comparison with the Expert model. The weaknesses of the Baseline model are its high communication, functional and project risks. Second, the Expert model has the smallest project duration, wait time, and communication and functional risks in comparison to the Baseline and the Hierarchical models. The weaknesses of the Expert model are the high levels of required rework, coordination and project risk. Third, the Hierarchy requires the least coordination and has the lowest level of project risk in comparison with the Baseline and the Expert model. In addition, the Hierarchy requires less rework in comparison to the Expert model. The Hierarchy's weaknesses are the project's duration, wait time, and communication and functional risks.

Hence, there is a set of tradeoffs that characterize these organization forms: to the extent that organizational speed is important. The Expert model appears to have an edge over the other two models, but to the extent that project risk represents a primary concern, the Hierarchy represents the sharper organization.

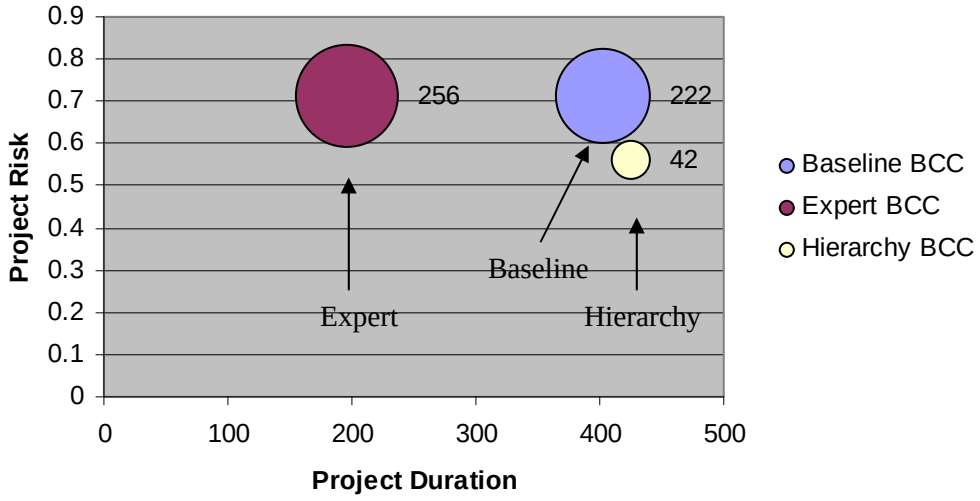

Figure 5. Project Duration, Risk and Required Coordination Comparison of the Models Under BCC

To illustrate this comparison it would be beneficial to take into account a key attribute of terrorist networks: the maintenance of a high secrecy level during the preparation and execution of an attack. When the actors, in order to accomplish a project, have to coordinate regularly, the secrecy of the project is put at risk. Therefore, in addition to the speed and project risk, coordination levels are of primary importance when examining terrorist groups. Figure 5 summarizes the project's risk, duration and coordination levels under BCC. The total amount of coordination required for each model is represented by the size of each circle, which has the exact coordination value (in person-days) next to it. Hence, a terrorist group that is risk averse and wants to maintain high level of secrecy (low coordination level) is more likely to have a hierarchical structure, and a group that has limited time to perform a task, and risk or required coordination is not of main concern, is more likely to have a decentralized form (Expert or Baseline, depending on the members' skill level).

B. HIGH COUNTERTERRORIST CONDITIONS' MODEL COMPARISON

When the Baseline, the Expert and the Hierarchical organizations are tested under high counterterrorist conditions (i.e., high levels of noise, task uncertainty and task complexity) the outcomes are the following. First, in the Baseline model under high counterterrorist conditions (HCC) the total project duration increases by 4 days (to 408 days), and the project duration of the Expert model remains almost the same (198 vs. 197 days). Moreover, the project duration for the Hierarchical model increases by 33 days (to 458 days) in comparison with the BCC. This differentiation between the two environments is affected by the different skill and application experience levels among the models, and the degree of change is a result of the model's structure. The Baseline and the Hierarchical models' actors have low skill and application experience levels and the Expert model's actors have high skill and experience levels. Tasks with great uncertainty and complexity under an environment with greater noise levels "slow down" amateur actors but have almost no effect, in terms of project duration, on expert actors. The total amount of rework is slightly greater for the Baseline (increase of four person-days) and the Expert (increase of two person-days) model and even greater for the

Hierarchical model (increase of 20 person-days) under HCC in comparison to BCC. The coordination is greater, in comparison with the BCC, for the Baseline (255 person-days), the Hierarchical (68 person-days) and the Expert (317 person-days) model. The wait time decreases slightly for both the Baseline (23 days) and Expert (three days) models but increases for the Hierarchy (84 days) model under HCC. The communication risk remains almost at the same levels for both the Baseline (0.61) and the Expert (0.56 vs. 0.55) models and slightly decreases for the Hierarchical (0.56) model under HCC. The functional and project risks remain almost the same for all three models under both counterterrorist conditions, indicating that extensive counterterrorist acts do not affect these variables. So all models (Baseline, Expert and Hierarchical models) outperform under BCC in terms of speed and required amounts of rework and coordination.

Therefore, there is a set of strengths and weaknesses that characterize these models under HCC. First, the Baseline model requires the smallest amount of rework in comparison with the other two models. Moreover, the Baseline model is faster and requires less wait time in comparison with the Hierarchical model. The weaknesses of the Baseline model are its high coordination level and its high communication, functional and project risk. Second, the Expert model has the smallest project duration, wait time, and communication and functional risks in comparison to the Baseline and the Hierarchical models. In addition, the Expert model requires less rework in comparison to the Hierarchy model. The weaknesses of the Expert model are the high levels of the required coordination and project risk. Third, the Hierarchy's strengths are the small amount of coordination and the low levels of communication and project risks in comparison with the Baseline and the Expert models. The Hierarchy's weaknesses are the project's duration, required rework, wait time and functional risk.

The results suggest that agencies that increase the counterterrorist activity (increased number of suspects' arrests and investigation of suspicious locations that may be used as meeting places for terrorists) do not increase the project risk involved in a terrorist project for both expert (Expert model) and amateur terrorist groups (Baseline and Hierarchical models). Moreover, high counterterrorist conditions delay the terrorist network's activities (Baseline, Expert and Hierarchical models) but the level of delay

depends on the terrorist group's structure and members' skill and application levels. HCC increase the Expert group's project duration by one day (almost 0.5%) and the amateur group's (Baseline model) project duration by four days (almost 1%). Therefore, higher counterterrorist conditions have almost no effect on the speed of decentralized groups. The hierarchy's project duration increases by 33 days (an almost 8% increase). Moreover, high counterterrorist conditions have little effect on the speed of a hierarchical group. In addition, HCC increase the required amount of coordination by almost 15% for the Baseline model, 24% for the Expert model and 62% for the Hierarchical model. Hence, the secrecy level of hierarchical terrorist groups is greatly decreased when the group operates under HCC. Figure 6 summarizes the comparison of the three models (Baseline, Expert and Hierarchy) in terms of speed, project duration and required coordination. The required coordination is represented by the size of each circle, which has the exact coordination value next to it.

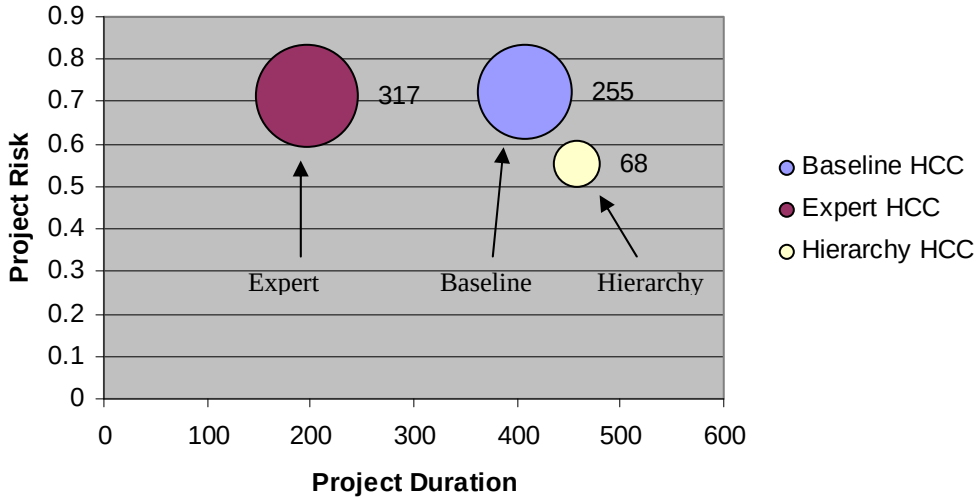

Figure 6. Project Duration, Risk and Required Coordination Comparison of the Models Under HCC

C. MODEL COMPARISON UNDER BOTH COUNTERTERRORIST CONDITIONS

Figure 7 illustrates the three models (Baseline, Expert and Hierarchy) under two counterterrorist conditions in terms of speed and risk. The Expert model is the fastest of

all models under both counterterrorist conditions, and the Hierarchy under both counterterrorist conditions (0.56 for BCC and 0.55 for HCC) has the lowest level of project risk.

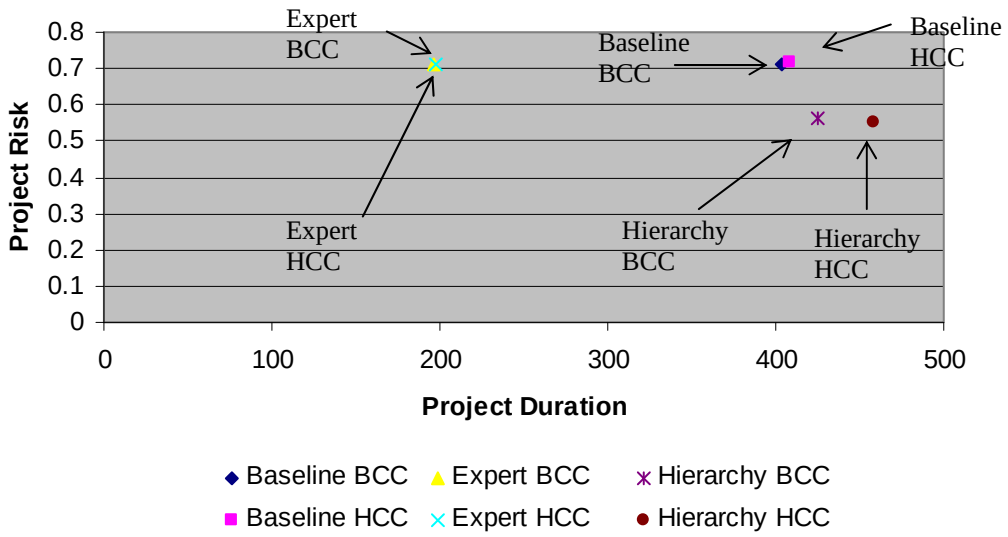

Figure 7. Project Duration and Risk Comparison Under Both Counterterrorist Conditions

To summarize, counterterrorist agencies should take into consideration the comparison of these three different terrorist configurations in order to understand their attributes and behavior under the two different counterterrorist environments. The organizational structure with greater speed is the decentralized terrorist network composed of experts, but when either the secrecy level or the project's risk is of main concern, the terrorist network with a hierarchical structure has an edge over the other two decentralized models. Therefore, counterterrorist agencies should focus primarily on decentralized terrorist networks (especially the ones composed of experts) when there are indications that a "terrorist attack project" might be planned and executed under tight time constraints. In addition, when time is not of primary concern for terrorist groups, but the maintenance of low levels of risk and coordination are, the hierarchical configuration of terrorist networks should be first examined by counterterrorist agencies.

When both secrecy and risk are of main concern to terrorists, and the terrorist group has a decentralized structure (based on information from intelligence sources), the terrorist groups composed of amateurs have an edge over a group composed of experts. Therefore, counterterrorist agencies should focus also on "amateur" groups because, even though the members of these groups lack skill and experience, they have shown in the past that they are capable of performing terrorist attacks (i.e., the 2004 Madrid train bombings).

Counterterrorist agencies should also take into consideration the fact that, in general, high counterterrorist conditions do not affect the project risk levels of the terrorist's project. In addition, under HCC, the required coordination among the members of decentralized terrorist networks (in both Baseline and Expert models) increases. In addition, the required level of coordination among hierarchical members increases significantly. Therefore, extensive counterterrorist conditions affect the secrecy level of all groups and especially of hierarchical configured networks. Moreover, the project duration of the hierarchical network increases by almost 8%. The Expert model's project duration remains almost the same and the Baseline's project duration increases almost by 1% within HCC in comparison with BCC. Thus, HCC affect the speed of hierarchical networks more than it affects the speed of decentralized networks. Hence, groups configured hierarchically are more "sensitive" to high counterterrorist conditions in comparison to decentralized terrorist networks. The conclusions, limitations and future research opportunities of this thesis are presented in Chapter VI.

VI. CONCLUSIONS

The understanding of terrorist networks is of main concern for governments, especially in the last decade, since major terrorist attacks, such as 9/11, the 2004 Madrid attack and the 2005 London attack, have changed people's view of security on their own soil. By implementing counterterrorist policies, governments try to safeguard their people and interests and thwart the terrorist cells that put them in danger.

Terrorism is a not a form of conventional warfare between states (e.g., World War II, Cold War) but a war between states and networks. Terrorism is not a regional phenomenon but a threat that exists at a global level (Robb, 2006). Terrorism is a network of networks that operates in a decentralized manner (Magouirk, et al., 2008). Bell (2002) suggests that thwarting terrorism requires a policy focusing on the fact that terrorism relies on commitment, so "loss of faith, the imposition of reality, and changing times can erode its strength." Brafman and Beckstrom (2006) similarly suggest that decentralized networks can be disrupted if their members lose the motivation that was the driving factor for them to join the network in the first place. On the other hand, terrorist networks are composed of individuals who can not be easily identified by the counterterrorist agencies, and this makes Bell's recommendation even more time consuming. Therefore, in order to analyze terrorist groups, counterterrorist agencies use various methods that help them understand terrorist groups in the short term, such as Social Network Analysis (SNA).

One of the uses of SNA methodology is to understand the relationships within terrorist networks (Hassan, 2007; Mccartan et al., 2008; Magouirk et al., 2008; Jordan et al., 2008). SNA is based on Network theory and examines the connections and interactions among individuals or groups based on common patterns of friendship, occupation, ethnicity, or any other pattern that is of interest to the researcher (Newman, 2003). The limitation of this approach is that it does not examine the structure and the workflow of the network for a specific activity (e.g., a bombing attack) and the types of interdependencies (sequential, reciprocal or pooled) that exist among the tasks. In

addition, it requires the identification of the individuals that compose a terrorist network, a task that is almost impossible to be performed before a terrorist attack or another incident.

Conceptual Simulation Models, using Agent Based Modeling, have been used to represent terrorist networks as business process and provide insights to counterterrorism policy makers (Leweling and Nissen, 2007). These computer-based models analyze terrorist networks primarily through the lens of contingency theory. This thesis examines the structure and the attributes of the terrorist network that was responsible for the 2004 Madrid bombing attack. It uses Agent Based Modeling to analyze the roles, activities and interdependencies of tasks and actors within the network, something that is not feasible through the use of Social Network Analysis. This approach generates new insights regarding the interdependencies of tasks related to a bombing attack, and examines how such a "project" could be slowed down if not disrupted.

The research design initially captures the Baseline model, which is an abstraction based on real world data from academic papers and news articles about the terrorist cell that performed the 2004 Madrid attack. The Baseline model is compared with SNA networks that represent the 2004 Madrid terrorist group, indicating the common general attributes that are derived from both models. The Baseline model represents a network of "amateurs," since its members had no previous experience with terrorist acts or any clear ties with the Al Qaeda network (Jordan and Wesley, 2006).

Then the Baseline model is compared with the Expert model, which is a representation of the Baseline model with highly trained and experienced members, and the Hierarchical model, which is a representation of the Baseline model with a hierarchical structure. This comparison is made to examine how different contingency factors affect the preparation and execution of a terrorist bombing attack. All models and comparisons are further examined under high counterterrorist conditions in order to test the networks' resilience when counterterrorist agencies increase the intensity of suspect arrests, investigations and surveillance.

All cases are simulated using POW-ER v.3.5b software, which is an Agent Based Model. The comparative results from the various tests mentioned above elucidate important insights into terrorist networks, suitable for advice to counterterrorist policy makers. Initially, terrorist organizations face a set of tradeoffs: to the extent that speed is of main concern, the decentralized terrorist network composed of experts represents the sharpest organizational form, but when either project risk or the required amount of coordination is of main concern, the terrorist network with a hierarchical structure has an edge over the other two decentralized structures. Therefore, counterterrorist agencies should take into consideration that, when time is not of main concern to terrorist organizations, hierarchical terrorist networks are able to perform an attack with the lowest level of project risk, maintaining at the same time the highest levels of secrecy. On the other hand, when it is known that terrorist networks are planning to perform an attack under time pressure, decentralized terrorist networks should be regarded as a primary threat. Hence, counterterrorist agencies, based on their intelligence sources about the terrorists' view of time, secrecy and project risk, could derive the possible structure of a terrorist network and conduct counterterrorist acts accordingly.

Moreover, high counterterrorist conditions do not affect the project risk of the terrorist's project. This applies to both hierarchical and decentralized terrorist networks. Hence, counterterrorist agencies should consider this limitation when they plan counterterrorist acts and consider it when they perform a cost benefit analysis for their counterterrorist policies.

In addition, extensive counterterrorist environments affect the secrecy level of all groups and especially of hierarchical configured networks. When agencies conduct extensive counterterrorist acts, the terrorists' secrecy level decreases. Even though HCC have no effect on project risk, they increase the required coordination among terrorists. This is an additional finding that counterterrorist agencies should take into consideration.

The project's duration of the hierarchical network also increases under HCC. The Expert model's speed remains almost the same and the Baseline's speed increases slightly within HCC in comparison with BCC. Hence, groups configured hierarchically are more "sensitive" to high counterterrorist conditions in comparison to decentralized

terrorist networks. Agencies should perform counterterrorist acts extensively when they face hierarchical terrorist groups since these actions decrease the network's speed and secrecy level. Counterterrorist agencies should have in mind that HCC have almost no effect on the decentralized terrorist network's speed and project risk but increase the required amount of coordination; therefore decrease the project's secrecy level.

In addition, decentralized (Edge-like) terrorist organizations face a set of tradeoffs: to the extent that organizational speed is important, a group composed of experts has an edge over a group of amateurs, but to the extent that risk represents a primary concern, both organizations appear appropriate. When, in addition to risk, the "project's" secrecy is of main concern, decentralized terrorist groups composed of amateurs have an edge over a decentralized terrorist group of experts. Therefore, counterterrorist agencies should focus also on "amateurs" because these groups may perform large-scale terrorist attacks (i.e., the 2004 Madrid train bombings).

This thesis has limitations that should be taken into consideration and delimit the generalization of this thesis. First, the Baseline model is an abstraction of the 2004 Madrid terrorist group. The Baseline model contains the key elements that are necessary for this study, excluding others that are of no central interest (Simon, 1996). Therefore, this model is not an exact imitation of reality, but rather an abstraction that focuses on specific areas of interest. Second, the results of this study are derived from the examination of a unique case study, the 2004 Madrid bombing attacks. According to Yin (2002) a cross examination of at least three case studies is necessary for theory development, followed by two more relative case studies for the validation of the derived theory. Therefore, the results from this case study should be compared with other similar studies in order to generalize counterterrorist suggestions and propositions. Third, in this thesis counterterrorist conditions are defined in terms of noise, task uncertainty and task complexity. Moreover, this thesis examines the 2004 Madrid bombings, which was a "successful" terrorist project, where no member of the group that is responsible for these attacks was captured before the attacks. Therefore, this thesis does not examine the underlying structure of a terrorist network that failed to perform an attack because of counterterrorist actions. Future research on "unsuccessful" terrorist attacks and the cross

comparison with “successful” ones would broaden our understanding of terrorist networks and the effect that counterterrorist acts have on them. Finally, the method of “backcasting” used in this study suggests that senior managers of the organization under study should inform the researchers whether or not their simulation outcomes are similar to those observed in reality. In this thesis, this was not possible since most of the members of the 2004 Madrid terrorist group have either died or are isolated in high security prisons. Instead, Social Network Analysis papers, along with newspaper articles and books that focused on the 2004 Madrid attack, were used to compare the Baseline model with the SNA models.

Using this thesis as a baseline, future research could examine terrorist networks that were responsible for other attacks, such as 9/11, the 2003 Bali attacks, and the 2005 London attacks. Such additional case studies can generate data and propositions that could be cross compared for the generation of more generally applicable counterterrorist propositions. Moreover, a similar approach could be used for the examination and analysis of other events that are performed by small groups, teams or even nations, taking into account that the researcher should be in a position to represent these groups in an organizational form performing specific tasks.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Alberts, D. S., & Hayes, R. E. (2003). *Power to the edge.* Command and Control Research Program, Washington, D.C.: CCRP Publication Series.

Arquilla, J. (1996). *The advent of netwar*. Washington, D.C.: RAND Corporation.

Atkinson, S. R. & Moffat, J. (2005). *The agile organization: From informal networks to complex effects and agility.* Command and Control Research Program, Washington, D.C.: CCRP Publication Series.

Barabási, A. L. (2002). *Linked: The new science of networks.* Cambridge, MA: Perseus Publishing.

BBC News. (2003, May 17). *Terror blasts rock Casablanca*. Retrieved June 30, 2008, from http://news.bbc.co.uk/1/hi/world/africa/3035803.stm

BBC News. (2004, March 12). *Madrid attacks timeline*. Retrieved June 30, 2008, from http://news.bbc.co.uk/2/hi/europe/3504912.stm

BBC News. (2004, April 4). *Timeline: Madrid investigation*. Retrieved July 1, 2008, from http://news.bbc.co.uk/2/hi/europe/3597885.stm

BBC News. (2004, April 4). *Madrid 'ringleader' dies in blast*. Retrieved July 1, 2008, from http://news.bbc.co.uk/1/hi/world/europe/3598219.stm

BBC News. (2004, April 5). *Piercing together Madrid bomber's past*. Retrieved July 1, 2008, from http://news.bbc.co.uk/2/hi/europe/3600421.stm

BBC News. (2005, March 10). *Madrid bombing suspects*. Retrieved July 1, 2008, from http://news.bbc.co.uk/2/hi/europe/3560603.stm

Bennhold, K. (2004, April 5). *Main suspect in Spain blasts among dead*. New York Times. Retrieved July 1, 2008, from http://query.nytimes.com/gst/fullpage.html?res=9F04EED71139F936A35757C0A9629C8B63&sec=&spon=&pagewanted=all

Bell, J. (2002). The organization of Islamic terror: The global jihad. *Journal of Management Inquiry*, *11*(3), 261-266.

Benjamin, D. & Simon, S. (2005). *The next attack: The failure of the war on terror and a strategy for getting it right.* New York: Times Books.

Bin Hassan, Muhammad Haniff Imam Samudra. (2007). Justification for Bali bombing. *Studies in Conflict & Terrorism*, *30*(12), 1033-1056.

Borshchev, A., & Filippov, A. (2004). From system dynamics and discrete event to practical agent based modeling: Reasons, techniques, tools. *The 22nd International Conference of the System Dynamics Society*. Oxford, England. Retrieved July 1, 2008, from http://www.systemdynamics.org/conferences/2004/SDS_2004/PAPERS/381BORSH.pdf

Brafman, O. & Beckstrom, R. A. (2006). *The starfish and the spider: The unstoppable power of leaderless networks.* New York: Portfolio Press.

Burton, R. M., & Obel, B. (1995). The validity of computational models in organization science. *Computational & Mathematical Organization Theory, 1*(1), 57-71.

Burton, R. M., & Obel, B. (2003). Computational laboratories for organization science: Questions, validity and docking. *Computational & Mathematical Organization Theory, 9*, 91-108.

Carley, K., & Prietula, M. (1994). *Computational organization theory*. Hillsdale, NJ: Lawrence Earlbaum Associates.

Cheng, C. H., & Levitt, R. E. (2001). Contextually changing behavior in medical organizations. *Proceedings of the 2001 Annual Symposium of the American Medical Informatics Association*. Washington, D.C.

Christiansen, T. R., (1993). Modeling Efficiency and Effectiveness of Coordination in Engineering Design Teams (Doctoral dissertation, Department of Civil and Environmental Engineering, Stanford University, 1993).

Epstein, J., & Axtell, R. (1996). *Growing artificial societies: Social science from the bottom up.* Washington, D.C. and Cambridge, MA: The Brookings Institution and the MIT Press.

Galbraith, J. (1977). *Organization Design*. Massachusetts: Addison Wesley Publishing Company.

Gateau, J. B., et al. (2007, June). Hypothesis testing of edge organizations: Modeling the C2 organization design space. *Proceedings International Command and Control Research and Technology Symposium*, Newport, Rhode Island.

Haahr-Escolano, K. (2005, July 1). Assessing Spain's al-Qaeda network. *Terrorism Monitor III* (13). Retrieved July 3, 2008, from http://www.jamestown.org/terrorism/news/article.php?issue_id=3388

Jin, Y., & Levitt, R. E. (1996). The virtual design team: A computational model of project organizations. *Journal of Computational and Mathematical Organizational Theory 2*(3), 171-195.

Jordan, J. E., Mañas F. M., & Horsburgh, M. (2008, January). Strengths and weaknesses of grassroot jihadist networks: The Madrid bombings. *Studies in Conflict & Terrorism 31*(1), 17-39.

Koons, J., Bekatoros N., & Nissen, M. E. (2008, June). C2 for computer networked operations: Using computational experimentation to identify effects on performance in organizational configurations within the larger network-centric environment. *Proceedings Command and Control Research Symposium.* Seattle, WA.

Kunz, J. C., Levitt, R. E., & Jin, Y. (1998). The virtual design team: A computational simulation model of project organizations. *Communications of the ACM*. *41*(11), 84-92.

Levitt, R. E., Thompsen, J., Christiansen, T. R., Kunz, J. C., Jin, Y., & Nass, C. (1999). Simulating project work processes and organizations: Toward a micro-contingency theory of organizational design. *Management Science. 45*(11), 1479-1495.

Looney, J. P. & Nissen, M. E. (2006, June). Computational modeling and analysis of networked organizational planning in a coalition maritime strike environment. *Proceedings Command and Control Research Symposium.* San Diego, CA.

March, J.G. &. Simon, H.A. (1958). *Organizations*. New York, Wiley Press.

Magouirk, J., Atran S., & Sageman, M. (2008). Connecting terrorist networks. *Studies in Conflict & Terrorism 31*(1), 1-16.

Mccartan, L. M., Masselli, A., Rey, M., & Rusnak, D. (2008). The logic of terrorist target choice: An examination of Chechen rebel bombings from 1997-2003. *Studies in Conflict & Terrorism 31*(1), 60-79.

Miller, J. H. & Page, S. E. (2007). *Complex adaptive systems*. Princeton, NJ: Princeton University Press.

Milgram, S. (1967). The small world problem. *Physiology Today 2,* 60-67.

Mintzberg, H. (1980). Structure in 5's: A synthesis of the research on organization design. *Management Science 26*(3), 322-341.

Mitroff, I. J. (1995). *The unbounded mind: Breaking the chains of traditional business thinking.* Oxford: Oxford University Press.

Mitroff, I. I., & Turoff. (1973, March). The whys behind the hows: Effective application of the many forecasting methods requires a grasp of their underlying philosophies. *IEEE Spectrum*, 62-71.

Napoleoni, L. (2005). *Insurgent Iraq: Al Zarqawi and the new generation.* New York: Seven Stories Press.

Newman, M. E. J. (2003). The structure and function of complex networks. *Society for Industrial and Applied Mathematics 45*(2), 167-256.

Nissen, M. & Levitt, R. E. (2004). Agent-based modeling of knowledge dynamics. *Knowledge Management Research & Practice 2*, 169-183.

Nissen, M. E. (2005a, June). Hypothesis testing of edge organizations: Specifying computational C2 models for experimentation. *Proceedings International Command and Control Research Symposium*. McLean, VA.

Nissen, M. E. (2005b, June). A computational approach to diagnosing misfits, inducing requirements, and delineating transformations for edge organizations. *Proceedings International Command and Control Research and Technology Symposium*, McLean, VA.

Nissen, M. E., Leweling, T. (2007). Defining and exploring the terrorism field: Toward an intertheoretic, agent-based approach. *Decision Support Systems 74*, 165-192.

Orr, R. J., & Nissen, M.E. (2006, September). Computational experimentation on C2 models. *Proceedings International Command and Control Research and Technology Symposium*, Cambridge, UK.

Ramsey, M. S. & Levitt, R. E. (2005, June). A Computational Framework for Experimentation with Edge Organizations, *Proceedings 10th International Command and Control Research and Technology Symposium,* Washington, D.C.

Robb, J. (2007). *Brave new war.* New Jersey: John Wiley & Sons, Inc.

Rodriguez, J. A. (2004). *The March 11th terrorist network: In its weakness lies its strength.* (Working Papers EPP-LEA, University of Barcelona).

Scholl, H. J. (2001). Agent-based and system dynamics modeling: A call for cross study and joint research. *34th Annual Hawaii International Conference on System Sciences 3*, 3003.

Sciolino E. & Horowitz, J. (2004, July 12). The talkative terrorist on tape: The Madrid plot was my project. *New York Times*. Retrieved July 3, 2008, from http://query.nytimes.com/gst/fullpage.html?res=9C07E4D8113BF931A25754C0A9629C8B63&sec=&spon=&pagewanted=print

Scott, W. R. (2001). *Institutions and organizations* (2nd ed.). Thousand Oaks, CA: Sage.

Simon, H. (1996). *The sciences of the artificial* (3rd ed.). Cambridge, MA: MIT Press.

Sterman, J.D. (2000). *Business dynamics: Systems thinking and modeling for a complex world*. Boston: Irwin McGraw-Hill.

Thompson, J. D. (1967). *Organizations in action*. New Jersey: Transaction Publishers.

Thomsen, J. (1998) *The virtual team alliance (VTA): Modeling the effects of goal incongruency in semi-routine, fast-paced project organizations* (Doctoral dissertation, Stanford University, 1998).

Yahoo News. (2008, August 4) *Instant messaging world confirms six degrees of separation*. Retrieved August 5, 2008, from http://news.yahoo.com/s/afp/20080805/tc_afp/usitinternetsocialmicrosoftoffbeat

Yin, R. K. (2002). *Case study research: Design and methodology* (3rd ed.). Thousand Oaks, CA: Applied Social Research Methods Series Volume 5.

Wiemann, G. (2006). *Terror on the internet.* Washington, DC: United States Institute of Peace Press.

Wright, L. (2004, August 2). The terror web. *The New Yorker*. Retrieved July 3, 2008 from, http://www.newyorker.com/archive/2004/08/02/040802fa_fact

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California